ELSEVIER Theoretical Computer Science 139 (1995) 275–314

Theoretical Computer Science

Observational specifications and the indistinguishability assumption

Gilles Bernot, Michel Bidoit*, Teodor Knapik

LIENS, C.N.R.S. U.R.A. 1327, Ecole Normale Supérieure, 45 Rue d'Ulm, F-75230 Paris Cedex 05, France

Communicated by M. Nivat
Received January 1992; revised December 1993

Abstract

To establish the correctness of some software w.r.t. its formal specification is widely recognized as a difficult task. A first simplification is obtained when the semantics of an algebraic specification is defined as the class of all algebras which correspond to the correct realizations of the specification. A software is then declared correct if some algebra of this class corresponds to it. We approach this goal by defining an **observational satisfaction relation** which is less restrictive than the usual satisfaction relation. Based on this notion we provide an institution for observational specifications. The idea is that the validity of an equational axiom should depend on an **observational equality**, instead of the usual equality. We show that it is not reasonable to expect an observational equality to be a congruence. We define an **observational algebra** as an algebra equipped with an observational equality which is an equivalence relation but not necessarily a congruence.

We assume that two values can be declared indistinguishable when it is impossible to establish they are different using some available observations. This is what we call the **Indistinguishability Assumption**. Since term observation seems sufficient for data type specifications, we define an indistinguishability relation on the carriers of an algebra w.r.t. the observation of an arbitrary set of terms. From a careful case study it follows that this requires to take into account the continuations of suspended evaluations of observation terms. Since our indistinguishability relation is not transitive, it is only an intermediate step to define an observational equality. Our approach is motivated by several examples.

1. Introduction

A main purpose of formal specifications is to provide a rigorous basis for establishing software correctness. Indeed, it is well known that proving the correctness of some piece of software without any formal reference makes no sense. Algebraic specifications are widely advocated as being one of the most promising formal specification

*Corresponding author. Email: [bernot, bidoit, knapik] @dmi.ens.fr.

SSDI 0304-3975(94)00017-D

techniques. However, to be provided with some algebraic specification is not sufficient per se. A precise (and adequate) definition of software correctness is mandatory. This crucial prerequisite must be first fulfilled before one can develop the relevant verification methods, and try to mechanize them.

The adequacy of the chosen definition of software correctness has a great practical impact, and we should therefore define software correctness according to the practical needs. In the framework of algebraic specifications, straightforward definitions of correctness turn out to be oversimplified: most programs that should be considered as being correct (from a practical point of view) are rejected. The first task is then to formally define the class of algebras which correspond to the correct implementations of a given specification. It is well known that this class should not only contain all the models of the specification but also some algebras which do not satisfy (in the usual sense) all axioms of the specification.[1] In fact, this class should rather correspond to the algebras which satisfy them "up to observations". For this reason, in our approach, we loosen the too restrictive usual satisfaction relation, in order to obtain an observational satisfaction relation "$\dot{\models}$", more permissive than "$\models$" in the sense that $\dot{\models}$ contains $\models$.

We consider an observation as an experiment which consists in computing some results given some inputs. In nonobservational approaches nothing is assumed about which kind of experiments is authorized and by default, this corresponds to the situation where everything may be observed. Notice that we will also use ambiguously the term "observation" when referring to the description of what are available experiments.

Assume now that the elements of some data type can only be observed by means of some available experiments. In this situation, it may well be impossible to distinguish some data type elements from others. This fact can be reflected by an indistinguishability relation, written "$\sim$", defined on a carrier of an algebra according to the following **Indistinguishability Assumption**:

Two values are indistinguishable with respect to some observations when it is impossible to establish that they are different, using these observations.

Now, the idea to loosen the satisfaction relation is to use "$\sim$" instead of "$=$" in the definition of the satisfaction relation. The usual satisfaction $A \models (t = t')$ of an equational axiom is based on the identity "$=$" of the results of the evaluation of both t and t′ in A, while an observational satisfaction should be based on whether these results are indistinguishable (i.e. related by "$\sim$") or not. Then the crucial point is to define the "$\sim$" relation, according to the Indistinguishability Assumption. Obviously, such a relation does not coincide with "$=$". Unlike in [16], [19] or [8] but similarly to [1] and [23] we want to consider more general observations than sort observation since

[1] The usual implementation of stacks by array-pointers is considered as correct. However, in general this implementation does not correspond to a model of the stack specification.

sort observation does not provide a satisfactory expressive power[2] (as shown in [14] or [17]). Unfortunately, an indistinguishability relation defined w.r.t. such general observations is not a congruence in general (see [23]). It may even not be an equivalence relation. As a matter of fact, according to the Indistinguishability Assumption, the observations only allow to decide that two elements should be distinct but not necessarily to decide tat they are equal. We overcome this problem by introducing an observational equality "$\cong$" included in "$\sim$". This leads us to the concept of observational algebras which are of the form $\langle A, \cong \rangle$ where A is an algebra (in the usual sense) equipped with an equivalence relation $\cong$.

We discuss the conditions under which our framework can provide an institution [6,7]. A first obvious condition is to let observations be part of some institution component. Since the observations act on the semantics of a specification in the same way as the axioms, we believe that the observations should be attached to the sentences part. Besides observational algebras, we also introduce observational sentences which are of the form $\langle \varphi, \mathrm{W} \rangle$ with φ a (usual) sentence and W a set of observation terms attached to it. In order to define an institution in such an approach, we investigate the relations between the variance (σ-translation, with σ a signature morphism) of observational sentences and the corresponding covariance ("σ-reduct") of observational algebras.

The approach we develop in this paper attempts to extend the class of the models of an algebraic specification by loosening the satisfaction relation. On the other hand there are approaches where this extension is made by means of an equivalence relation $\equiv_{\mathrm{Obs}}$ on algebras (called **behavioural equivalence**) depending on some observations Obs [18, 22, 15, 11, 16, 21]. In these approaches, the class of "observational models" (also called behaviours), denoted by **Beh[SP, Obs]**, which should correspond to the correct realization of a specification SP, is usually defined in the following way:

$$\mathrm{Beh}[\mathrm{SP}, \mathrm{Obs}] = \{B \in \mathrm{Alg}[\mathrm{Sig}[\mathrm{SP}]] \mid \exists A \in \mathrm{Alg}[\mathrm{SP}],\ A \equiv_{\mathrm{Obs}} B\} \tag{1.i}$$

Based on this notion, in [21] Sannella and Tarlecki have developed an institution-independent framework.

Even if very general, in our opinion, these approaches do not provide a satisfactory observational semantics. It turns out that there exist some realizations that we would like to consider as being correct, but unfortunately these realizations cannot be shown to be behaviourally equivalent to any of the (usual) models of the specification at hand. A limit-case example of such a situation, namely when $\mathrm{Alg}[\mathrm{SP}] = \emptyset$, is given in the next section.

[2] Sort observation is not precise enough, in the sense that it may be necessary to observe less than all the (reachable, observationally reachable) values of a given sort.

2. Beyond sort observation

Let SWC (see Fig. 1) be a usual specification of sets of natural numbers with an additional operation choose : Set→Nat, defined by the axiom $s \neq \emptyset \Rightarrow choose(s) \in s =$ true. By this axiom we require choose to return an arbitrary element of any nonempty set. Consider a usual algebra L of lists of natural numbers. Clearly, lists behave like sets if we only observe them via the membership operation. For this reason we can consider L as an "observational model" of SWC, choose being realized by car. In this realization the lists nm and mn (with $n \neq m$) are indistinguishable, since they are viewed as the same set $\{n, m\}$. However $choose(nm)$ and $choose(mn)$ produce two Nat values which should be distinguishable. Accordingly, we should not request the indistinguishability relation to be a congruence. Once admitted, this claim has an immediate and important consequence: if the observational satisfaction of an equation $l = r$ depends on the indistinguishability relation, an algebra may observationally satisfy $l = r$, without satisfying $f(l) = f(r)$. Consequently an inconsistent specification in the usual sense) may be considered as "observationally consistent" provided that the inconsistencies are not observed. For instance, in Fig. 1, sets of natural numbers with an operation enum, which enumerates a set into a list, have been specified in a very natural way. Unfortunately this specification is inconsistent in the usual sense. Thus in the approaches based on behavioural equivalence, from (1.i), we have $Beh[SP, Obs] = \emptyset$ for any set of observations Obs. On the contrary, in an approach with an observational satisfaction relation this specification can have models (sets can be realized by lists, enum being the identity), provided that the inconsistencies are not observed

spec: SWC
use: NAT, BOOL
sort: Set
operations:
$\emptyset$: →Set
ins: Nat Set→Set
$\_\in\_$: Nat Set→Bool
del : Nat Set→Set
choose : Set→Nat
axioms:
ins(x, ins(x, s)) = ins(x, s)
ins(x, ins(y, s)) = ins(y, ins(x, s))
del(x, $\emptyset$) = $\emptyset$
del(x, ins(x, s)) = del(x, s)
$x \neq y \Rightarrow$ del(x, ins(y, s)) = ins(y, del(x, s))
$x \in \emptyset$ = false
$x \in$ ins(x, s) = true
$x \neq y \Rightarrow x \in$ ins(y, s) = $x \in s$
$s \neq \emptyset \Rightarrow$ choose(s) $\in$ s = true

spec: SWE
use: LIST, NAT, BOOL
sort: Set
operations:
$\emptyset$: →Set
ins : Nat Set→Set
$\_\in\_$: Nat Set→Bool
del : Nat Set→Set
enum : Set→List
axioms:
ψ_1: ins(x, ins(x, s)) = ins(x, s)
ψ_2: ins(x, ins(y, s)) = ins(y, ins(x, s))
ψ_3: del(x, $\emptyset$) = $\emptyset$
ψ_4: del(x, ins(x, s)) = del(x, s)
ψ_5: $x \neq y \Rightarrow$ del(x, ins(y, s)) = ins(y, del(x, s))
ψ_6: $x \in \emptyset$ = false
ψ_7: $x \in$ ins(x, s) = true
ψ_8: $x \neq y \Rightarrow x \in$ ins(y, s) = $x \in s$
ψ_9: enum($\emptyset$) = nil
ψ_{10}: enum(ins(x, s)) = cons(x, enum(s))

Fig. 1. Specification of sets with choose and with enum.

(i.e. enum cannot occur in observation terms). Moreover, the latter aim cannot be achieved in a satisfactory way using sort observation. It is clear that in this example we want to observe e.g. s(s(0)) but not car(enum(ins(s(s(0)), $\emptyset$))) while with sort observation we can observe either both or none.[3] Given two computations which yield the same result (e.g. car(cons(s(s(0)), nil)) and car(enum(ins(s(s(0)), $\emptyset$)))) we can choose the set of observation terms so that one computation is observed (e.g. the first one) and the other (e.g. the second one) is not. This points out the advantage of term observation with respect to sort observation. The latter allows to observe values but not computations [17]. Moreover sort observation is not expressive enough when values which have to be observed do not fit to whole carriers (e.g. we may want to observe a strict subset of a carrier of Nat, such as a given interval). Examples are given in Section 11.

As a summary we state the following claims:

1. *An observational equality depends on observations. Since these are proper to a data type, each data type has its own observational equality.*
2. *The operations do not necessarily preserve observational equalities* (*i.e.* "$\sim$" *is not necessarily a congruence*).
3. *Two distinguishable elements cannot be equal. Two indistinguishable elements are not necessarily equal.*

3. Basic definitions

We assume that the reader is familiar with algebraic specifications (see e.g. [5] or [9] and [24]). A **signature** Σ consists of a finite set S of **sort symbols** and a finite set of **operation names with arities** ambiguously denoted by Σ. We assume that each signature Σ is extended with an S-sorted set of variables X such that X_s is countable for each $s \in S$. We use the following conventions. Given a signature Σ (resp. Σ'), S (resp. S') denotes the sorts of Σ (resp. of Σ') and X (resp. X') denotes the variables of the extended Σ (resp. of Σ'). A **signature morphism** $\sigma : \Sigma \to \Sigma'$ maps each sort of S to a sort of S', and each operation $(f : s_1 \ldots s_n \to s) \in \Sigma$ to an operation $\sigma(f)$ of Σ' with the arity $\sigma(s_1) \ldots \sigma(s_n) \to \sigma(s)$ and is extended by an injective map on variables that sends each variable of X_s to a variable of $X'_{\sigma(s)}$. Note that we assume that a signature morphism is always injective on variables.[4] Signatures with signature morphisms form the usual category of signatures, written **Sig**.

From $T_\Sigma(X)$ (the S-sorted set of $\Sigma(X)$-terms, i.e. terms on the extended signature $\Sigma(X)$), the "=" symbol, propositional connectives ($\neg$, $\vee$, $\wedge$, $\Rightarrow$, etc.) and quantifiers

[3] More precisely, sort observation allows to split carriers among observed and unobserved. Accordingly a term is then considered as observed if its sort is observable.

[4] Without this assumption, which under a stronger form appears in [7, Definition 58, p. 136], it would be impossible to establish the satisfaction condition for most institutions.

$(\forall, \exists)$ we construct the set of **well-formed Σ-formulae** and the set $\mathbf{Wfs}[\Sigma]$ of **well-formed Σ-sentences** (which are Σ-formulae with no free variable) in the usual way. The definition of **(total) Σ-algebras** and (algebraic) **Σ-morphisms** is the standard one, as well as the satisfaction relation between Σ-algebras and Σ-sentences. The **category of all Σ-algebras** is denoted by $\mathbf{Alg}[\Sigma]$. Given an S-sorted set E, we denote by $\mathbf{T}_\Sigma(\mathbf{E})$ the free Σ-algebra over E. For instance $\mathbf{T}_\Sigma$ (resp. $\mathbf{T}_\Sigma(\mathbf{X})$) denotes the **$\Sigma$-algebra of ground terms** (resp. **terms with variables**), $\mathbf{T}_\Sigma(A)$ (resp. $\mathbf{T}_\Sigma(A \cup \mathbf{X})$) denotes the **$\Sigma$-algebra of ground terms** (resp. **terms with variables) over the carriers of a Σ-algebra** A, or free algebra over A, for short. Given a signature morphism $\sigma: \Sigma \to \Sigma'$, the **$\sigma$-reduct** of a Σ'-algebra A', written $A'_{|\sigma}$ is defined in the usual way, and extending this on Σ'-morphisms we obtain the **forgetful functor** $-_{|\sigma}: \mathrm{Alg}[\Sigma'] \to \mathrm{Alg}[\Sigma]$. In the particular case of an inclusion $\Sigma \subseteq \Sigma'$ (that is, of an inclusion signature morphism $\sigma: \Sigma \hookrightarrow \Sigma'$), the corresponding forgetful functor is written $-_{|\Sigma}$.

Definition 3.1. A **substitution** ρ is an S-sorted map from X to an S-sorted set E such that $\rho_s: X_s \to E_s$ is

total iff $E_s = \emptyset \Rightarrow X_s = \emptyset$

everywhere undefined iff $E_s = \emptyset$ and $X_s \neq \emptyset$.

A **valuation** v from X to an algebra A is a substitution from X to $A \cup X$ such that $v_s = \mathrm{Id}_{X_s}$ whenever $A_s = \emptyset$. The set of all valuations from X to A is written $\mathbf{Val}[\mathbf{X}, A]$. A **partial valuation** v from X to A is a substitution from X to $A \cup X$ such that if $v(x) \in X$ then $v(x) = x$.

From the freeness of $T_\Sigma(X)$ any valuation (resp. partial valuation) v followed by the S-sorted inclusion $A \subseteq T_\Sigma(A)$ (resp. $A \subseteq T_\Sigma(A \cup X)$) extends to a unique morphism (ambiguously written v) from $T_\Sigma(X)$ to $T_\Sigma(A \cup X)$ that maps each term $t \in (T_\Sigma(X))_s$ to a **(partially) valued term** $tv \in (T_\Sigma(A \cup X))_s$. Notice that if $A_s \neq \emptyset$ for each $s \in S$ then for all $v: X \to A$ and all $t \in T_\Sigma(X)$, $tv \in T_\Sigma(A)$. We say then that tv is **(totally) valued**. The **evaluation morphism** from $T_\Sigma(A)$ to A is defined as the unique Σ-morphism which maps each element of $T_\Sigma(A)_s \cap A_s$ to itself. This morphism maps a valued term τ to its **evaluation result** written $\bar{\tau}$.

A **position** p in a term t is a sequence of integers which describe the path from the topmost position of t (denoted by the empty sequence) to the **subterm of t at position p** written $\mathbf{t}_{|p}$. The set of all positions of t is denoted by **Pos(t)**. The replacement of $t_{|p}$ by a term r in t is written $\mathbf{t}[\mathbf{r}]_p$. The multiple replacement at parallel positions $p_1, \ldots, p_n$ is written $\mathbf{t}[\mathbf{r}_1 \ldots \mathbf{r}_n]_{p_1 \ldots p_n}$.

Definition 3.2. Given sorts $S = \{s_1, \ldots, s_n\}$ the **set of contextual variables** is the (S-*indexed*) set $\Diamond = \{\diamond_{s_1}, \ldots, \diamond_{s_n}\}$ with $\{\diamond_{s_i}\}$ called the **contextual variable of sort s_i**. A **context** over a Σ-algebra A is a partially valued term η with only one contextual

variable and no other variable. Consequently, the S-sorted set of all contexts over A, written $\mathbf{C}_\Sigma(A)$, is defined as follows:

$$C_\Sigma(A)=\bigcup_{s\in S} T_\Sigma(A\cup\{\diamond_s\})$$

Given $\eta\in C_\Sigma(A)$ we can write $\eta:s\to s'$ instead of $\eta\in(T_\Sigma(A\cup\{\diamond_s\}))_{s'}$. Application of $\eta:s\to s'$ on $a\in A_s$ is written $\eta[a]$.

The following definitions are very technical as well as subsequent results of this section. They can therefore be skipped at first reading.

Definition 3.3. Given a signature morphism $\sigma:\Sigma\to\Sigma'$ and a Σ'-algebra A', we define $\overline{\sigma_{A'}}$ as the unique application from $A'_{|\sigma}$ to A', which maps each element of $(A'_{|\sigma})_s$ to the equal element of $A'_{\sigma(s)}$, for all $s\in S$.

Definition 3.4. Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism, A' be a Σ'-algebra. We define $\sigma_{A'}:T_\Sigma(A'_{|\sigma})\to T_{\Sigma'}(A')$ as the unique extension of both $\overline{\sigma_{A'}}:A'_{|\sigma}\to A'$ and $\sigma:T_\Sigma\to T_{\Sigma'}$.

Definition 3.5. Given a signature morphism $\sigma:\Sigma\to\Sigma'$ and a Σ'-algebra A', we define a **σ-reduct of a valuation** $v':X'\to A'$ as a valuation $v'_{|\sigma}:X\to A'_{|\sigma}$ satisfying

$$\begin{aligned}&\forall s\in S\ \forall x\in X_s \quad A'_{\sigma(s)}\neq\emptyset \Rightarrow \sigma(x)v'=\overline{\sigma_{A'}}(xv'_{|\sigma})\\ &\forall s\in S\ \forall x\in X \quad A'_{\sigma(s)}=\emptyset \Rightarrow xv'_{|\sigma}=x.\end{aligned}\tag{3.i}$$

We also use the pointwise extension of this definition to sets of valuations, that is $\Upsilon'_{|\sigma}$ stands for $\{v'_{|\sigma}\mid v'\in\Upsilon\}$, for any $\Upsilon'\subseteq Val[X',A']$.

Notice that this definition makes sense, since σ and $\overline{\sigma_{A'}}$ are well defined. The notation $v'_{|\sigma}$ suggests that the relation $-_{|\sigma}$ defined on the valuations by Eq. (3.i) is a function. The following lemma points out this fact.

Lemma 3.6. *Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism and A' be a Σ'-algebra. The relation $-_{|\sigma}$ defined by Eq. (3.i) is a total and surjective function $-_{|\sigma}:Val[X',A']\to Val[X,A'_{|\sigma}]$.*

Proof. *Functionality*:
Let $v':Val[X',A']$. We show that there exists a unique $v:X\to A'_{|\sigma}$ such that $\sigma(x)v'=\overline{\sigma_{A'}}(xv)$.

Assume that $\sigma(x)v'=a'$ for $x\in X_s$. Since $\sigma(s)$ is the sort of $\sigma(x)$, by definition of valuation $a'\in A'_{\sigma(s)}$. Since σ is not necessarily injective on the sorts, $\sigma_{A'}^{-1}(a')=\{a_1,\ldots,a_n\}$, each a_i having different sort of $\sigma^{-1}(\sigma(s))$. Thus, there exists the unique a_k of the sort s. The valuation v, we are looking for, exists and maps x into its unique value a_k. Consequently v is unique.

Surjectivity: We show that for all $v: X \to A'_{|\sigma}$ there exists $v': \mathrm{Val}[X', A']$ such that $v'_{|\sigma} = v$.

Let $x' \in X'$. If $x' \notin \sigma(X)$ we do not need to care about $x'v'$. Let then $x' \in \sigma(X)$. Since σ is injective on variables there exists, a unique $x \in X$ s.t. $\sigma(x) = x'$. If $xv = x$ then according to Definition 3.5, $x'v' = x'$. Let therefore $xv = a$, $a \in A'_{|\sigma}$. Then the value which v' should map to x' exists and is equal to $\overline{\sigma_{A'}}(a)$. This proves the existence of v'. □

Lemma 3.7. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism and A' be a Σ'-algebra. For any valuation $v': X' \to A'$ and any term $t \in T_\Sigma(X)$ such that $\sigma(t)v' \in T_{\Sigma'}(A')$ we have*

$$\overline{\sigma(t)v'} = \overline{\sigma_{A'}}(\overline{tv'_{|\sigma}})$$

Proof. Obvious, since according to Definition 3.4 we have $\sigma(t)v' = \sigma_{A'}(tv'_{|\sigma})$ and $\overline{\sigma_{A'}(tv'_{|\sigma})} = \overline{\sigma_{A'}}(\overline{tv'_{|\sigma}})$. □

Corollary 3.8. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism and A' be a Σ'-algebra. For any valued term $\tau \in T_\Sigma(A'_{|\sigma})$ we have*

$$\overline{\sigma_{A'}(\tau)} = \overline{\sigma_{A'}}(\bar{\tau})$$

Proof. It is a trivial consequence of Lemma 3.7 since τ can always be written $tv'_{|\sigma}$ with $t \in T_\Sigma(X)$ and $v': X' \to A'$ (see Lemma 3.6). □

4. How to observe and how to compare

As mentioned in the introduction we are going to define an indistinguishability relation on the carriers of an algebra in order to relax the satisfaction relation. Usually this is done using the concept of observable contexts. Since this concept was only defined for sort [8, 10, 15, 16] or signature[5] [1, 23] observations, we should start by defining it for the case where we observe an arbitrary set of terms. We first need two preliminary definitions. Deep motivations of all definitions of this section are given in [2].

Definition 4.1. Let A be a Σ-algebra. We define the **partial evaluation relation**, written $\xrightarrow[\mathrm{pEv}]{}$, on $T_\Sigma(A)$ as follows. We say that a term $\tau_2 \in T_\Sigma(A)$ is a result of partial evaluation of $\tau_1 \in T_\Sigma(A)$, written $\tau_1 \xrightarrow[\mathrm{pEv}]{} \tau_2$, if there is a position p in τ_1 such that $\tau_1[\overline{\tau_1|_p}]_p = \tau_2$.

Fact 4.2. *The reflexive-transitive closure of $\xrightarrow[\mathrm{pEv}]{}$, written $\xrightarrow[\mathrm{pEv}]{*}$, is a partial order.*

[5] In fact these approaches combine signature and sort observations.

Definition 4.3. Let $W \subseteq T_\Sigma(X)$ be a set of terms and A be a Σ-algebra. The **closure by partial evaluations of W in A**, written $\tilde{W}^A$, is defined as follows:

$$\tilde{W}^A = \{\tau \in T_\Sigma(A) \mid \exists w \in W\ \exists v : X \to A\ wv \xrightarrow[pEv]{*} \tau\}$$

This leads to the definition of observable contexts.

Definition 4.4. Let $W \subseteq T_\Sigma(X)$ be a set of observation terms and a be an element of a Σ-algebra A. We say that a context $\eta \in C_\Sigma(A)$ is a **W-observable context of a** (an observable context of a, for short) if $\eta[a] \in \tilde{W}^A$. The set of W-observable contexts of a is written $\mathbf{cont}_W(a)$. (If there is no ambiguity we omit the index W in this notation.)

The above definition provides an answer to the question of how to observe an element of a carrier of an algebra. It is clear from this definition that, given a set of observation terms W, such an element a can be observed through its W-observable contexts. The next definitions provide an answer to the question of how to compare two elements a and b of a carrier of an algebra.

Definition 4.5. A **W-comparator** (comparator, for short) of elements a and b of a given carrier of a Σ-algebra is any W-observable context of both a and b. The set of all comparators of a and b is denoted by $\mathbf{cmp}_W(a, b)$. (If there is no ambiguity we omit the index W in this notation.) We say that a W-comparator η **distinguishes** a and b iff $\overline{\eta[a]} \neq \overline{\eta[b]}$.

With the latter it is natural to define an indistinguishability relation as follows.

Definition 4.6. We say that two elements a and b of a given carrier of a Σ-algebra are **indistinguishable** w.r.t. a set of terms $W \subseteq T_\Sigma(X)$ (or **W-indistinguishable**), written $a \sim_W b$, if there is no W-comparator which distinguishes them.

We illustrate the concepts introduced so far by means of the specification SWE (see Fig. 1).

Example 4.7. Let Γ_{SWE} be the signature of SWE except the enum operation. Consider the following set of observation terms $Obs_{SWE} = (T_{\Gamma_{SWE}}(X))_{Bool} \cup (T_{\Gamma_{SWE}}(X))_{Nat}$. Assume that we enrich SWE with the operation idl : List → List defined by the axiom idl(l) = l. (This operation, without any practical interest, aims at precisely define an algebra as a σ-reduct of another one.) Since SWE is an enrichment of LIST we can write

$$Sig[SWE] = Sig[LIST] + \Delta\Sigma$$

Then we consider the following signature morphism:

$$\sigma = \sigma_{LIST} + \Delta\sigma \quad \text{with } \sigma_{LIST} : Sig[LIST] \to Sig[LIST]$$

$$\Delta\sigma : \Delta\Sigma \to Sig[LIST]$$

where σ_{LIST} is the identity morphism and

$$\Delta\sigma(\mathsf{Set})=\mathsf{List} \quad \Delta\sigma(\emptyset)=\mathsf{nil} \quad \Delta\sigma(\mathsf{ins})=\mathsf{cons}$$

$$\Delta\sigma(\in)=\mathsf{member} \quad \Delta\sigma(\mathsf{del})=\mathsf{remove} \quad \Delta\sigma(\mathsf{enum})=\mathsf{idl}$$

Consider the Sig[LIST]-algebra L being the usual realization of lists. Then the Sig[SWE]-algebra we are interested in is $L_{|\sigma}$. The observable contexts of $l\in(L_{|\sigma})_{\mathsf{List}}$ are the following ones:

$$\mathrm{cont}(l)=\{\mathsf{car}(\eta), \mathsf{member}(n,\eta) \mid n\in(L_{|\sigma})_{\mathsf{Nat}},\ \eta\in(\mathrm{C}_{\Gamma_{\mathsf{SWE}}}(L_{|\sigma}))_{\mathsf{List}}\}$$

Therefore, $\sim_{\mathrm{Obs}_{\mathsf{SWE}}}$ is the identity on $(L_{|\sigma})_{\mathsf{LIST}}$. The observable contexts of $s\in(L_{|\sigma})_{\mathsf{Set}}$ are the following ones:

$$\mathrm{cont}(s)=\{n\in\eta \mid n\in(L_{|\sigma})_{\mathsf{Nat}},\ \eta\in(\mathrm{C}_{\Gamma_{\mathsf{SWE}}}(L_{|\sigma}))_{\mathsf{Set}}\}$$

Thus $s, s'\in(L_{|\sigma})_{\mathsf{Set}}$ are indistinguishable if they contain the same elements.

We would like to propose an institution for observational specifications. Since our observational satisfaction relation (which will be defined later) strongly depends on observable contexts, we must first study their properties w.r.t. the forgetful functor and the translation of observation terms. In this way, we are going to provide tools which will be useful to show that the satisfaction condition holds in our framework. Below we give the first important theorem. It is a good opportunity to establish some interesting lemmas about partial evaluation.

Theorem 4.8. *Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism, $\mathrm{W}\subseteq\mathrm{T}_{\Sigma}(\mathrm{X})$ and $\mathrm{W}'\subseteq\mathrm{T}_{\Sigma'}(\mathrm{X}')$ be sets of terms such that $\sigma(\mathrm{W})\subseteq\mathrm{W}'$ and A' be a Σ'-algebra. For any element $a\in A'_{|\sigma}$ and any context $\eta\in\mathrm{C}_{\Sigma}(A'_{|\sigma})$ we have*

$$\eta\in\mathrm{cont}_{\mathrm{W}}(a) \Rightarrow \sigma_{A'}(\eta)\in\mathrm{cont}_{\mathrm{W}'}(\overline{\sigma_{A'}}(a))$$

We need the following lemmas for the proof.

Lemma 4.9. *Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism, and A' be a Σ'-algebra. For all $\tau_1,\tau_2\in\mathrm{T}_{\Sigma}(A'_{|\sigma})$ we have*

$$\tau_1 \xrightarrow[\mathrm{pEv}]{} \tau_2 \Rightarrow \sigma_{A'}(\tau_1)\xrightarrow[\mathrm{pEv}]{}\sigma_{A'}(\tau_2)$$

Proof. By Definition 4.1 there exists a position $\mathrm{p}\in\mathrm{Pos}(\tau_1)$ such that $\tau_1[\overline{\tau_1|_{\mathrm{p}}}]_{\mathrm{p}}=\tau_2$. By Corollary 3.8 we have

$$\overline{\sigma_{A'}}(\overline{\tau_1|_{\mathrm{p}}})=\overline{\sigma_{A'}(\tau_1|_{\mathrm{p}})}=\overline{\sigma_{A'}(\tau_1)|_{\mathrm{p}}}$$

Hence

$$\sigma_{A'}(\tau_2)=\sigma_{A'}(\tau_1[\overline{\tau_1|_p}]_p)=\sigma_{A'}(\tau_1)[\overline{\sigma_{A'}(\tau_1|_p)}]_p=\sigma_{A'}(\tau_1)[\overline{\sigma_{A'}(\tau_1)|_p}]_p$$

This proves $\sigma_{A'}(\tau_1)\xrightarrow[pEv]{}\sigma_{A'}(\tau_2)$. □

Lemma 4.10. *Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism, and A' be a Σ'-algebra. For any $\tau_1,\tau_2\in T_\Sigma(A'_{|\sigma})$ we have*

$$\tau_1\xrightarrow[pEv]{*}\tau_2 \Rightarrow \sigma_{A'}(\tau_1)\xrightarrow[pEv]{*}\sigma_{A'}(\tau_2)$$

Proof. Follows directly from the previous lemma. □

Lemma 4.11. *Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism, $W\subseteq T_\Sigma(X)$ and $W'\subseteq T_{\Sigma'}(X')$ be sets of terms such that $\sigma(W)\subseteq W'$ and A' be a Σ'-algebra. For any $\tau\in T_\Sigma(A'_{|\sigma})$ we have*

$$\tau\in\tilde{W}^{A'_{|\sigma}} \Rightarrow \sigma_{A'}(\tau)\in\tilde{W}'^{A'}$$

Proof. Assume $\tau\in\tilde{W}^{A'_{|\sigma}}$. By Definition 4.3 we have

$$\exists w\in W\ \exists v:X\to A'_{|\sigma}\quad wv\xrightarrow[pEv]{*}\tau$$

By Lemma 4.10 we obtain

$$\exists w\in W\ \exists v:X\to A'_{|\sigma}\ \sigma_{A'}(wv)\xrightarrow[pEv]{*}\sigma_{A'}(\tau) \tag{i}$$

By Lemma 3.6 we know that there exists a valuation $v':X'\to A'$ such that $v'_{|\sigma}=v$. It is obvious from Definition 3.5 that $\sigma_{A'}(wv)=\sigma(w)v'$. Consequently, from (i), we deduce

$$\exists w\in W\ \exists v':X\to A'\quad \sigma(w)v'\xrightarrow[pEv]{*}\sigma_{A'}(\tau)$$

Now $\sigma(w)\in W'$, hence

$$\exists w'\in W'\ \exists v':X\to A'\quad w'v'\xrightarrow[pEv]{*}\sigma_{A'}(\tau)$$

By Definition 4.3 this yields $\sigma_{A'}(\tau)\in\tilde{W}'^{A'}$. □

Proof of Theorem 4.8. Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism, $W\subseteq T_\Sigma(X)$ and $W'\subseteq T_{\Sigma'}(X')$ be sets of terms such that $\sigma(W)\subseteq W'$ and A' be a Σ'-algebra. Let $a\in A'_{|\sigma}$.

Assume $\eta\in\mathrm{cont}_W(a)$. By Definition 4.4 we have $\eta[a]\in\tilde{W}^{A'_{|\sigma}}$, hence by Lemma 4.11 we deduce $\sigma_{A'}(\eta[a])\in\tilde{W}'^{A'}$. By Definition 4.4 this yields $\sigma_{A'}(\eta)\in\mathrm{cont}_{W'}(\overline{\sigma_{A'}}(a))$. □

Notice that the converse of the above theorem does not hold even if $\sigma(W)=W'$.

Example 4.12. Consider the following signatures:

$$\Sigma=\{f_1,f_2:s\to s\}\qquad \Sigma'=\{f':s'\to s'\}$$

Let $W=\{f_1(x)\}$. Let $\sigma:\Sigma\to\Sigma'$ be the following signature morphism:

$$\sigma(s)=s' \qquad \sigma(f_1)=\sigma(f_2)=f'$$

It is clear that for any Σ'-algebra A', $f_2(\diamond)$ is not a W-observable context of any element $a\in A'_{|\sigma}$, whereas $\sigma(f_2(\diamond))=f'(\diamond)\in \mathrm{cont}_{\sigma(W)}(\overline{\sigma_{A'}}(a))$.

The above example shows that in some situations $\sigma(W)$ can generate more observations than W. In such a situation we may have $a\sim_W b$ and $\overline{\sigma_{A'}}(a)\not\sim_{\sigma(W)}\overline{\sigma_{A'}}(b)$. More generally the converse of Lemma 4.11 does not hold in this situation. It is possible to overcome this problem by imposing the following syntactic condition on W and σ:

$$\sigma^{-1}(\sigma(W))=W$$

If W and σ satisfy this property then the converse of Lemma 4.11 holds for the particular case $\sigma(W)=W'$. This is stated as follows.

Lemma 4.13. *Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism and $W\subseteq T_\Sigma(X)$ and $W'\subseteq T_{\Sigma'}(X')$ two sets of terms such that $\sigma^{-1}(W')=W$. Let A' be a Σ'-algebra. For all $\tau\in T_\Sigma(A'_{|\sigma})$ and all $\tau'\in T_{\Sigma'}(A')$ such that $\overline{\sigma_{A'}}(\tau)=\tau'$ we have*

$$\tau\in\tilde{W}^{A'_{|\sigma}} \Leftrightarrow \tau'\in\tilde{W}'^{A'}$$

Proof. Let $\tau\in T_\Sigma(A'_{|\sigma})$ and $\tau'\in\tilde{W}'^{A'}$ such that $\tau'=\sigma_{A'}(\tau)$. By Definition 4.3 this is equivalent to

$$\exists w'\in W' \ \exists v':X'\to A' \quad w'v'\xrightarrow[pEv]{*}\tau'$$

Since $\sigma^{-1}(W')=W$ the above formula is equivalent to

$$\exists w\in W \ \exists v':X'\to A' \quad \sigma(w)v'\xrightarrow[pEv]{*}\tau' \tag{i}$$

According to Definition 3.5 it is obvious that $\sigma_{A'}(wv'_{|\sigma})=\sigma(w)v'$. Consequently, we can consider $v=v'_{|\sigma}$. Due to the hypothesis that $\sigma_{A'}(\tau)=\tau'$, formula (i) is then equivalent to

$$\exists w\in W \ \exists v:X\to A'_{|\sigma} \quad \sigma_{A'}(wv)\xrightarrow[pEv]{*}\sigma_{A'}(\tau)$$

By Lemma 4.10 this is equivalent to

$$\exists w\in W \ \exists v:X\to A'_{|\sigma} \quad wv\xrightarrow[pEv]{*}\tau$$

By Definition 4.3 this is equivalent to $\tau\in\tilde{W}^{A'_{|\sigma}}$. □

Under the same hypothesis of Lemma 4.13 the converse of Theorem 4.8 holds. We have then an equivalence instead of an implication.

Theorem 4.14. *Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism, $W\subseteq T_\Sigma(X)$, $W'\in T_{\Sigma'}(X')$ be two sets of terms such that $\sigma^{-1}(W')=W$ and A' be a Σ'-algebra. For any $a\in A'_{|\sigma}$ and any*

$\eta \in C_\Sigma(A'_{|\sigma})$ and $\eta' \in C_{\Sigma'}(A')$ such that $\sigma_{A'}(\eta)=\eta'$ we have

$$\eta \in \mathrm{cont}_W(a) \Leftrightarrow \eta' \in \mathrm{cont}_{W'}(\overline{\sigma_{A'}}(a))$$

Proof. Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism, $W \subseteq T_\Sigma(X)$ and $W' \subseteq T_{\Sigma'}(X')$ be two sets of terms such that $\sigma^{-1}(W')=W$ and A' be a Σ'-algebra. Let $a \in A'_{|\sigma}$, $\eta \in C_\Sigma(A'_{|\sigma})$ and $\eta' \in C_{\Sigma'}(A')$ such that $\sigma_{A'}(\eta)=\eta'$.

Assume $\eta \in \mathrm{cont}_W(a)$. Due to Definition 4.4 this is equivalent to $\eta[a] \in \tilde{W}^{A'_{|\sigma}}$, and by Lemma 4.13 is equivalent to

$$\sigma_{A'}(\eta[a]) \in \tilde{W}'^{A'} \tag{i}$$

It is clear that $\sigma_{A'}(\eta[a])=\sigma_{A'}(\eta)[\overline{\sigma_{A'}}(a)]$. Due to the hypothesis that $\sigma_{A'}(\eta)=\eta'$, formula (i) is therefore equivalent to

$$\eta'[\overline{\sigma_{A'}}(a)] \in \tilde{W}'^{A'}$$

which by Definition 4.4 is equivalent to $\eta' \in \mathrm{cont}_{W'}(\overline{\sigma_{A'}}(a))$. □

5. Properties of the indistinguishability relation

Definition 4.6 expresses in which situations two elements of a Σ-algebra are indistinguishable w.r.t. a given set of observations. Indeed, it defines an S-sorted relation $\sim_W=(\sim_W)_{s\in S}$ on an algebra, called the **indistinguishability relation**. Since this relation is the next step toward a complete description of our institution for observational specifications, we must study its properties w.r.t. the forgetful functor and the translation of observation terms. This will be necessary for establishing the satisfaction condition (see [7]) in a further section. After the following proposition devoted to this aim, we study other interesting properties of the indistinguishability relation.

Proposition 5.1. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism, let $W \subseteq T_\Sigma(X)$ and $W' \subseteq T_{\Sigma'}(X')$ be sets of terms such that $\sigma(W) \subseteq W'$ and A' be a Σ'-algebra. For all $s \in S$, for all $a', b' \in A'_{\sigma(s)}$ and $a, b \in (A'_{|\sigma})_s$ such that $\overline{\sigma_{A'}}(a)=a'$ and $\overline{\sigma_{A'}}(b)=b'$ we have*

$$a' \sim_{W'} b' \Rightarrow a \sim_W b$$

Proof. Let $a', b' \in A'_{\sigma(s)}$ such that $a' \sim_{W'} b'$. Assume by contradiction that there exist $a, b \in (A'_{|\sigma})_s$ such that

$$\overline{\sigma_{A'}}(a)=a' \qquad \overline{\sigma_{A'}}(b)=b' \quad \text{and} \quad a \not\sim_W b$$

According to Definition 4.6 there exists $\eta \in \mathrm{cmp}_W(a, b)$ such that

$$\overline{\eta[a]} \neq \overline{\eta[b]} \tag{i}$$

By definition of comparator (see Definition 4.5) η is an element of $\mathrm{cont}_{\mathrm{W}}(a)$ and $\mathrm{cont}_{\mathrm{W}}(b)$. On the other hand, it is clear that

$$\sigma_{A'}(\eta)[a'] = \sigma_{A'}(\eta[a]) \quad \text{and} \quad \sigma_{A'}(\eta)[b'] = \sigma_{A'}(\eta[b]) \tag{ii}$$

From Corollary 3.8 we have therefore

$$\overline{\sigma_{A'}(\eta[a])} = \overline{\sigma_{A'}}(\overline{\eta[a]}) \quad \text{and} \quad \overline{\sigma_{A'}(\eta[b])} = \overline{\sigma_{A'}}(\overline{\eta[b]}) \tag{iii}$$

From (i), (ii) and (iii) we obtain

$$\overline{\sigma_{A'}(\eta)[a']} \neq \overline{\sigma_{A'}(\eta)[b']} \tag{iv}$$

Now, from Theorem 4.8 we know that $\sigma_{A'}(\eta)$ is an element of $\mathrm{cont}_{\mathrm{W}'}(a')$ (resp. $\mathrm{cont}_{\mathrm{W}'}(b')$). Accordingly, it is a comparator of a' and b' and by (iv) it distinguishes a' and b'. This is in contradiction with the starting hypothesis. □

As for observable contexts in the previous section we would like to have an equivalence between $\overline{\sigma_{A'}}(a) \sim_{\mathrm{W}'} \overline{\sigma_{A'}}(b)$ and $a \sim_{\mathrm{W}} b$. A sufficient condition is again $\sigma^{-1}(\mathrm{W}') = \mathrm{W}$.

Proposition 5.2. *Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\mathrm{W} \subseteq \mathrm{T}_{\Sigma}(\mathrm{X})$ and $\mathrm{W}' \subseteq \mathrm{T}_{\Sigma'}(\mathrm{X}')$ be two sets of terms such that $\sigma^{-1}(\mathrm{W}') = \mathrm{W}$ and let A' be a Σ'-algebra. For all $a, b \in (A'_{|\sigma})_{\mathrm{s}}$ we have*

$$\overline{\sigma_{A'}}(a) \sim_{\mathrm{W}'} \overline{\sigma_{A'}}(b) \Leftrightarrow a \sim_{\mathrm{W}} b$$

Proof. Let $a, b \in (A'_{|\sigma})_{\mathrm{s}}$ such that $a \sim_{\mathrm{W}} b$. By Definition 4.5 this is equivalent to

$$\forall \eta \in \mathrm{cmp}_{\mathrm{W}}(a, b) \quad \overline{\eta[a]} = \overline{\eta[b]}$$

Since $\overline{\sigma_{A'}}$ is injective when restricted to one sort and $\mathrm{cmp}_{\mathrm{W}}(a, b) = \mathrm{cont}_{\mathrm{W}}(a) \cap \mathrm{cont}_{\mathrm{W}}(b)$, the above formula is equivalent to

$$\forall \eta \in \mathrm{cont}_{\mathrm{W}}(a) \cap \mathrm{cont}_{\mathrm{W}}(b) \quad \overline{\sigma_{A'}}(\overline{\eta[a]}) = \overline{\sigma_{A'}}(\overline{\eta[b]})$$

According to Corollary 3.8 this is equivalent to

$$\forall \eta \in \mathrm{cont}_{\mathrm{W}}(a) \cap \mathrm{cont}_{\mathrm{W}}(b) \quad \overline{\sigma_{A'}(\eta)[\overline{\sigma_{A'}}(a)]} = \overline{\sigma_{A'}(\eta)[\overline{\sigma_{A'}}(b)]} \tag{i}$$

From the hypothesis that $\sigma^{-1}(\mathrm{W}') = \mathrm{W}$ we deduce that any W′-observable context is an element of $\mathrm{C}_{\sigma(\Sigma)}(A')$. Now, for all $\eta' \in \mathrm{C}_{\sigma(\Sigma)}(A')$ there exists $\eta \in \mathrm{C}_{\Sigma}(A'_{|\sigma})$ such that $\sigma_{A'}(\eta) = \eta'$. Hence using Theorem 4.14 we deduce that formula (i) is equivalent to

$$\forall \eta' \in \mathrm{cont}_{\mathrm{W}'}(\overline{\sigma_{A'}}(a)) \cap \mathrm{cont}_{\mathrm{W}'}(\overline{\sigma_{A'}}(b)) \quad \overline{\eta'[\overline{\sigma_{A'}}(a)]} = \overline{\eta'[\overline{\sigma_{A'}}(b)]}$$

By Definition 4.5 this is equivalent to $\overline{\sigma_{A'}}(a) \sim_{\mathrm{W}'} \overline{\sigma_{A'}}(b)$. □

As a corollary of Proposition 5.1, we have the following fact which makes clear the antimonotonicity character of the indistinguishability relation w.r.t. the inclusion of sets of observation terms.

Corollary 5.3. *Let* W_1, W_2 *be two sets of* Σ*-terms such that* $W_1 \subseteq W_2$. *On any* Σ*-algebra, the indistinguishability relations* $\sim_{W_1}$ *and* $\sim_{W_2}$ *satisfy* $\sim_{W_2} \subseteq \sim_{W_1}$.

Proof. It is enough to consider the previous proposition with $\Sigma = \Sigma'$, $W = W_1$, $W' = W_2$ and σ the identity. □

The following fact is obvious from the definition of the indistinguishability relation.

Fact 5.4. *The indistinguishability relation is reflexive and symmetric.*

The next fact fully agrees with our claims.

Fact 5.5. *The indistinguishability relation is not always compatible with operations.*

Proof. It is enough to go back to Example 4.7. Recall that in the algebra $L_{|\sigma}$, sets are represented by lists. Let then $\langle n, m\rangle$ and $\langle m, n\rangle$ be two representations of the set $\{n, m\}$ in this algebra. On the one hand we have $\langle n, m\rangle \sim_{\mathrm{Obs}_{\mathrm{SWE}}} \langle m, n\rangle$ but on the other hand $\mathsf{enum}^{L|\sigma}(\langle n, m\rangle) \not\sim_{\mathrm{Obs}_{\mathrm{SWE}}} \mathsf{enum}^{L|\sigma}(\langle m, n\rangle)$ because of the comparator $\mathsf{car}(\diamond)$ which distinguishes them. □

We have also a negative result.

Fact 5.6. *The indistinguishability relation is not transitive in general.*

Consider the model A (see Fig. 2) of the specification TRANS. In this algebra we have $\mathsf{a}^A \sim_W \mathsf{b}^A$ and $\mathsf{b}^A \sim_W \mathsf{c}^A$, but not $\mathsf{a}^A \sim_W \mathsf{c}^A$. The reason is that we did not impose any restriction on the set of observation terms. Consequently, nothing ensures that all the elements of a given data type can be observed in the same way. In the algebra A each of the elements $\mathsf{a}^A, \mathsf{b}^A, \mathsf{c}^A$ is observed differently, each pair among these elements is compared in some proper way, different from the others. This is the reason why the indistinguishability relation is not transitive. In fact, this property results directly from our Indistinguishability Assumption according to which we have built Definitions 4.6, 4.4 and 4.5. However, when all the elements of a given carrier of an algebra have the same observable contexts, the indistinguishability relation is transitive.

Fact 5.7. *Let* A *be a* Σ*-algebra and* W *be a set of* Σ*-terms. If* $\mathrm{cont}_W(a) = \mathrm{cont}_W(b)$ *for all* $a, b \in A_s$ *then the relation* $\sim_W$ *is transitive on* A.

Proof. Obvious. □

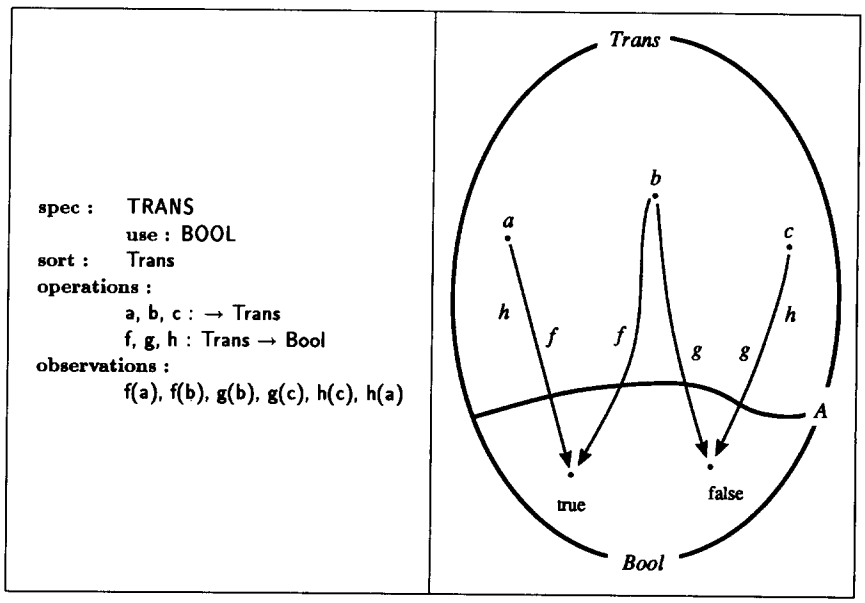

Fig. 2. Specification TRANS and one of its models.

It is possible to have a definition of "$\sim_W$" which is always transitive. One may state that a and b are W-indistinguishable if they do in the sense of Definition 4.6 and if additionally $\mathrm{cont}_W(a) = \mathrm{cont}_W(b)$. In our opinion, such a definition will distinguish too much. For instance, if in a specification we observe only some **ground** terms then, according to Definition 4.6, a nonreachable value will never be distinguished from any other value, whereas with the modified version of this definition, a nonreachable value will always be distinguished from any reachable value. Consequently we are not enthusiastic about such a modification.

Fact 5.8. *The relation* $\sim_{\mathrm{Obs}_{SWE}}$ *from Example* 4.7 *is transitive.*

Proof. Follows directly from Fact 5.7, since in Example 4.7 we have shown that the elements of the same carrier of $L_{|\sigma}$ have the same observable contexts. □

Fact 5.7 provides a semantical transitivity criterion of the indistinguishability relation. There exist also some syntactical criteria. We describe them in the next section.

6. A particular case of term observation

An interesting case arises when the set of observation terms is described by a *partial subsignature* defined precisely by the following definition.

Definition 6.1. Let Σ be a signature. **A partial subsignature of Σ** (partial signature for short) is a pair $\langle S_1, \Sigma_0 \rangle$ such that Σ_0 is a subsignature of Σ and S_1 is a subset of sorts of Σ_0. The set of terms $T_{\langle S_1, \Sigma_0 \rangle}(X)$ of a partial signature $\langle S_1, \Sigma_0 \rangle$ (the set of $\langle S_1, \Sigma_0 \rangle$-terms) is defined as follows:

$$T_{\langle S_1, \Sigma_0 \rangle}(X) = \coprod_{s \in S_1} (T_{\Sigma_0}(X))_s.$$

This kind of sets of terms is interesting because the indistinguishability relation generated by such a set on any Σ-algebra is transitive. In order to make this point clear, we first introduce an auxiliary definition of $\langle S_1, \Sigma_0 \rangle$-*indistinguishability*. This is a transitive relation. We show then that this relation is the same as $T_{\langle S_1, \Sigma_0 \rangle}(X)$-indistinguishability (in the sense of Definition 4.6). This last result allows one to conclude that any $T_{\langle S_1, \Sigma_0 \rangle}(X)$-indistinguishability is transitive on all Σ-algebras.

Definition 6.2. Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ and A be a Σ-algebra. We say that $a, b \in A_s$ are $\langle S_1, \Sigma_0 \rangle$-indistinguishable, written $a \sim_{\langle S_1, \Sigma_0 \rangle} b$, if for any term $t \in T_{\langle S_1, \Sigma_0 \rangle}(X)$ with at least one variable x_s of sort s and for all valuations $\nu_1, \nu_2 \in \mathrm{Val}[X, A]$ which satisfy $t\nu_1, t\nu_2 \in T_\Sigma(A)$ and which coincide everywhere except at x_s where $x_s\nu_1 = a$ and $x_s\nu_2 = b$, we have

$$\overline{t\nu_1} = \overline{t\nu_2}$$

Proposition 6.3. *Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ. The relation of $\langle S_1, \Sigma_0 \rangle$-indistinguishability is transitive on all Σ-algebras.*

Proof. Consider $a, b, c \in A_s$ such that $a \sim_{\langle S_1, \Sigma_0 \rangle} b$ and $b \sim_{\langle S_1, \Sigma_0 \rangle} c$. From Definition 6.2, this amounts to saying that $\overline{t\nu_1} = \overline{t\nu_2} = \overline{t\nu_3}$ for any term $t \in T_{\langle S_1, \Sigma_0 \rangle}(X)$ and all the valuations $\nu_1, \nu_2, \nu_3 \in \mathrm{Val}[X, A]$ which coincide everywhere except at an $x_s \in \mathrm{Var}[t]$ where $x_s\nu_1 = a$, $x_s\nu_2 = b$ and $x_s\nu_3 = c$. Hence, we deduce immediately that

$$a \sim_{\langle S_1, \Sigma_0 \rangle} c \qquad \square$$

Theorem 6.4. *Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ and A be a Σ-algebra. For all $a, b \in A_s$ we have*

$$a \sim_{\langle S_1, \Sigma_0 \rangle} b \quad \textit{iff} \quad a \sim_{T_{\langle S_1, \Sigma_0 \rangle}(X)} b$$

The proof of this theorem requires a technical definition as well as some additional results.

Definition 6.5. Let A be a Σ-algebra and $\tau \in T_\Sigma(A)$ be a valued term. Consider the following set of positions:

$$\{p_1, \ldots, p_n\} = \{p \in \mathrm{Pos}(\tau) \mid \tau|_p \in A\}$$

We call a term $t \in T_\Sigma(X)$ **τ-derived**, if it is obtained from τ by replacement of all its leaves at positions $p_1, \ldots, p_n$ by distinct variables. In other words $t = \tau[x_1, \ldots, x_n]_{p_1 \ldots p_n}$ with $x_i \neq x_j$ when $i \neq j$. We let **der(τ)** denote the set of all τ-derived terms.

Lemma 6.6. *Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ, t be a term of $T_{\langle S_1, \Sigma_0 \rangle}(X)$, A be a Σ-algebra and $v: X \to A$ be a valuation. If $tv \xrightarrow[pEv]{*} \tau$, where $\tau \in T_\Sigma(A)$, then* $der(\tau) \subseteq T_{\langle S_1, \Sigma_0 \rangle}(X)$.

Proof. Obvious, since the sort of any term of $der(\tau)$ is in S_1 and every operator occurring in it is in Σ_0, according to Definitions 4.1 and 6.5. □

Lemma 6.7. *Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ and A be a Σ-algebra. For all $\tau \in \widetilde{T_{\langle S_1, \Sigma_0 \rangle}(X)}^A$ we have*

$$der(\tau) \subseteq T_{\langle S_1, \Sigma_0 \rangle}(X)$$

Proof. Assume $\tau \in \widetilde{T_{\langle S_1, \Sigma_0 \rangle}(X)}^A$. By Definition 4.3 we have

$$\exists t \in T_{\langle S_1, \Sigma_0 \rangle}(X)\ \exists v: X \to A \quad tv \xrightarrow[pEv]{*} \tau$$

Hence, by Lemma 6.6 we deduce that $der(\tau) \subseteq T_{\langle S_1, \Sigma_0 \rangle}(X)$. □

Lemma 6.8. *Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ and a be an element of a Σ-algebra A. For any $\eta \in cont_{T_{\langle S_1, \Sigma_0 \rangle}(X)}(a)$ we have*

$$der(\eta[a]) \subseteq T_{\langle S_1, \Sigma_0 \rangle}(X)$$

Proof. Assume $\eta \in cont_{T_{\langle S_1, \Sigma_0 \rangle}(X)}(a)$. By Definition 4.4 $\eta[a]$ is an element of $\widetilde{T_{\langle S_1, \Sigma_0 \rangle}(X)}^A$. Hence, applying Lemma 6.7, we obtain the result we are looking for. □

Lemma 6.9. *Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ, A be a Σ-algebra and let $a, b \in A_s$. For any $\eta \in cmp_{T_{\langle S_1, \Sigma_0 \rangle}(X)}(a, b)$ there exists a term $t \in T_{\langle S_1, \Sigma_0 \rangle}(X)$, and valuations $v_1, v_2 \in Val[X, A]$ which coincide everywhere except at $x_s \in Var[t]$ where $x_s v_1 = a$ and $x_s v_2 = b$ and such that $\eta[a] = tv_1$ and $\eta[b] = tv_2$.*

Proof. Let $\eta \in cmp_{T_{\langle S_1, \Sigma_0 \rangle}(X)}(a, b)$ and $t_0 \in der(\eta[a])$. It is obvious that $der(\eta[a]) = der(\eta[b])$, therefore $t_0 \in der(\eta[b])$. Let $\{p_1, \ldots, p_n\}$ be all positions of $\diamond_s$ in η and let $x_s \notin Var[t_0]$. Notice that $Pos(\eta) = Pos(t_0)$. Consequently, we can consider a term $t = t_0[x_s]_{p_1 \ldots p_n}$. Since by Lemma 6.8 t_0 is in $T_{\langle S_1, \Sigma_0 \rangle}(X)$, we also have $t \in T_{\langle S_1, \Sigma_0 \rangle}(X)$. By construction of t, there exists a valuation $v_1: X \to A$ such that $tv_1 = \eta[a]$. Hence $x_s v_1 = a$. It is obvious that there exists a valuation $v_2: X \to A$ which coincides with v_1 everywhere except at x_s where $x_s v_2 = b$. Then we are done since $tv_2 = \eta[b]$. □

Proof of Theorem 6.4. Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ and A be a Σ-algebra. We will proceed by an indirect proof. We show that for all $a, b \in A_s$ we have $a \not\sim_{\langle S_1, \Sigma_0 \rangle} b$ iff $a \not\sim_{T_{\langle S_1, \Sigma_0 \rangle}(X)} b$.

($\Rightarrow$) Let $a, b \in A_s$ such that $a \not\sim_{\langle S_1, \Sigma_0 \rangle} b$. By Definition 6.2, there exists a term $t \in T_{\langle S_1, \Sigma_0 \rangle}(X)$ and valuations $v_1, v_2 \in \mathrm{Val}[X, A]$ which coincide everywhere except at $x_s \in \mathrm{Var}[t]$ where $x_s v_1 = a$ and $x_s v_2 = b$, such that

$$\overline{tv_1} \neq \overline{tv_2} \tag{i}$$

Let $\{p_1, \ldots, p_n\}$ be the set of positions where x_s occurs in t. Consider then a context $\eta = tv_1[\diamond]_{p_1 \ldots p_n}$. It is obvious that $\eta = tv_2[\diamond]_{p_1 \ldots p_n}$ and that $\eta[a] = tv_1$ and $\eta[b] = tv_2$. Now, by Definition 4.3 we have $tv_1, tv_2 \in \overbrace{T_{\langle S_1, \Sigma_0 \rangle}(X)}^{A}$. So $\eta \in \mathrm{cmp}_{T_{\langle S_1, \Sigma_0 \rangle}(X)}(a, b)$ and according to (i), η distinguishes a and b, hence $a \not\sim_{T_{\langle S_1, \Sigma_0 \rangle}(X)} b$ by Definition 4.6.

($\Leftarrow$) Let $a, b \in A_s$ such that $a \not\sim_{T_{\langle S_1, \Sigma_0 \rangle}(X)} b$. By Definition 4.6, there exists $\eta \in \mathrm{cmp}_{T_{\langle S_1, \Sigma_0 \rangle}(X)}(a, b)$ such that

$$\overline{\eta[a]} \neq \overline{\eta[b]} \tag{ii}$$

But according to Lemma 6.9 there exists a term $t \in T_{\langle S_1, \Sigma_0 \rangle}(X)$, and valuations $v_1, v_2 \in \mathrm{Val}[X, A]$ which coincide everywhere except at $x_s \in \mathrm{Var}[t]$ where $x_s v_1 = a$ and $x_s v_2 = b$ and such that $\eta[a] = tv_1$ and $\eta[b] = tv_2$. From (ii) we deduce that $\overline{tv_1} \neq \overline{tv_2}$. Hence $a \not\sim_{\langle S_1, \Sigma_0 \rangle} b$, by Definition 6.2. □

Corollary 6.10. *Let $\langle S_1, \Sigma_0 \rangle$ be a partial subsignature of Σ. The relation of indistinguishability w.r.t. the set of terms $T_{\langle S_1, \Sigma_0 \rangle}(X)$ is transitive on all Σ-algebras.*

Proof. Follows immediately from Theorem 6.4 and Proposition 6.3. □

We give below an example of observation by a partial signature.

Example 6.11. Consider the observations $\mathrm{Obs}_{\mathsf{SWE}}$ from Example 4.7. Recall that $\mathrm{Obs}_{\mathsf{SWE}} = (T_{\Gamma_{\mathsf{SWE}}}(X))_{\mathsf{Bool}} \cup (T_{\Gamma_{\mathsf{SWE}}}(X))_{\mathsf{Nat}}$. In fact, this is an observation by a partial subsignature of Sig[SWE], namely $\langle \{\mathsf{Bool}, \mathsf{Nat}\}, \Gamma_{\mathsf{SWE}} \rangle$.

Partial signatures are used as observations in [1]. Observational equality w.r.t. $\langle S_1, \Sigma_0 \rangle$ defined in that paper coincides with our $\langle S_1, \Sigma_0 \rangle$-indistinguishability on all reachable algebras. However these two relations do not coincide on nonreachable algebras, not even on their reachable parts. If two elements are $\langle S_1, \Sigma_0 \rangle$-indistinguishable then they are also observationally equal w.r.t. $\langle S_1, \Sigma_0 \rangle$ (in the sense of [1]) but the converse is true only for reachable algebras. This is due to the fact that our comparators are elements of $C_\Sigma(A)$ while those used in [1] can be viewed as elements of C_Σ. Since $C_\Sigma \subseteq C_\Sigma(A)$ we have more possibilities than [1] to distinguish two elements.

7. Observational algebras

In Section 5 we have shown that the indistinguishability relation is not transitive in general. For this reason, an observational satisfaction relation cannot be directly based on the indistinguishability relation, in contrast with the usual satisfaction relation, which is based on the usual equality (of the elements of an algebra). Its nontransitive character (see Fact 5.6) would make it unusable as interpretation of an equivalence predicate. On the contrary, the noncongruence property (see Fact 5.5) does not entirely reject this possibility, provided that such exotic operations as enum (see Fig. 1) are treated with care. For instance in some term t of SWE we can replace its subterm $t|_p = \mathsf{ins}(\mathsf{s}(0), \mathsf{ins}(0, \emptyset))$ by $\mathsf{ins}(0, \mathsf{ins}(\mathsf{s}(0), \emptyset))$ except when there is some enum in t above the position p.[6] In addition, similarly to [23], we believe that there is no reason to expect an "observational equality" to be a congruence. This may happen only in the particular case of sort observation.

We can conclude that at this moment the only problem is due to the nontransitive character of the indistinguishability relation. For this reason, we introduce in this section the notion of observational equality which, being transitive, is a step toward an observational satisfaction relation.

At the end of Section 2 we have stated a few claims as the result of the former discussion. They now lead us to the following conclusions:

- Because of the second claim, an observational equality need not be a congruence for the same reason why the indistinguishability relation is not such, in general (see Fact 5.5).
- The last claim suggests that on a given algebra, an observational equality is not unique.
- The first claim suggests that observational equality should be an S-sorted relation.

Putting these conclusions together, we state the following definition.

Definition 7.1. Given a signature Σ, an **observational Σ-algebra** is a pair "$\langle A, \cong \rangle$" where A is a Σ-algebra and $\cong$ is an S-sorted equivalence relation on A, called **observational equality on A**. We let $\mathbf{OAlg}[\Sigma]$ denote the class of all observational Σ-algebras.

Notice that:

- A Σ-algebra A can be considered in a straightforward way as an observational Σ-algebra $\langle A, = \rangle$.
- In general we can form an infinity of observational algebras from a Σ-algebra. For this reason we use the notation $\cong^\alpha$ or $\cong^\beta$ in order to distinguish between two relations which form two observational algebras $\langle A, \cong^\alpha \rangle$ and $\langle A, \cong^\beta \rangle$ from a given algebra A.

[6] More precisely, this replacement is impossible only if each node on the path from p to the closest enum above p (if there is one) is of sort Set.

The reader certainly realizes that our definition of observational algebras is similar to the one of structures in first-order logic where each predicate symbol is interpreted by a relation. We consider the equality symbol "=" in the axioms as a particular predicate symbol. This symbol is explicitly interpreted in an observational algebra by its observational equality.

The term "equality" may seem somehow misleading in this context, since an observational equality is not necessarily a congruence. The term "observational equivalence" might be therefore more appropriate. Nevertheless, this may be confused with observational equivalence between algebras [21]. Consequently, in our approach, we keep the term "observational equality".

Example 7.2. Consider $L_{|\sigma}$ and $\mathrm{Obs}_{\mathsf{SWE}}$ both defined in Example 4.7. Since $\sim_{\mathrm{Obs}_{\mathsf{SWE}}}$ is an equivalence relation (see Fact 5.8), the pair $\langle L_{|\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}}\rangle$ is an observational Sig[SWE]-algebra.

Definition 7.3. An **observational Σ-morphism** $\mu:\langle A, \cong^A\rangle \to \langle B, \cong^B\rangle$ is any (usual) Σ-morphism from A to B which preserves the observational equality, i.e. for all $s\in S$:

$$\forall a,b\in A_s \quad a\cong^A b \Rightarrow \mu(a)\cong^B \mu(b)$$

It is obvious that OAlg[Σ] equipped with the observational Σ-morphisms forms a category.

Definition 7.4. Let $\sigma:\Sigma\to\Sigma'$ be a signature morphism. The **σ-reduct** of an observational Σ'-algebra $\langle A', \cong'\rangle$ is the observational Σ-algebra

$$\langle A', \cong'\rangle_{|\sigma} = \langle A'_{|\sigma}, \cong'_{|\sigma}\rangle$$

where $A'_{|\sigma}$ is the usual σ-reduct of the Σ'-algebra A' and $(\cong'_{|\sigma})_s = \cong'_{\sigma(s)}$ for all $s\in S$.

The mapping $-_{|\sigma}$ extends to observational morphisms as in the usual framework. Consequently, it defines the **forgetful functor** from OAlg[Σ'] to OAlg[Σ] associated to σ. Thus we can also view OAlg as a functor from the category of signatures Sig to the dual of the category of all categories $\mathrm{Cat}^{\mathrm{op}}$. OAlg maps each object Σ of Sig to the category of the observational Σ-algebras and each signature morphism σ to the corresponding forgetful functor $-_{|\sigma}$. Notice that this provides components upon which an institution can be built.

8. Validity of observational sentences

Before introducing observational sentences and defining their validity in observational algebras we give some additional definitions and results.

Definition 8.1. A **solution** of an equation $1=r$ in an observational Σ-algebra $\langle A, \cong \rangle$ is a (total) valuation $v: X \to A$ such that either $lv \notin T_\Sigma(A)$ or $rv \notin T_\Sigma(A)$ or $\overline{lv} \cong \overline{rv}$. The set of all the solutions of an equation is written $[\mathbf{l}=\mathbf{r}]_{\langle A, \cong \rangle}$. The set of solutions of a formula φ is defined recursively as follows:

- if $\varphi = \neg\psi$ then $[\varphi]_{\langle A, \cong \rangle} = \mathrm{Val}[X, A] \setminus [\psi]_{\langle A, \cong \rangle}$
- if $\varphi = \psi \wedge \psi'$ then $[\varphi]_{\langle A, \cong \rangle} = [\psi]_{\langle A, \cong \rangle} \cap [\psi']_{\langle A, \cong \rangle}$
- if $\varphi = \forall x \psi$ then

$$[\varphi]_{\langle A, \cong \rangle} = \{v \in \mathrm{Val}[X, A] \mid \forall \mu \in \mathrm{Val}[X, A]\ (\forall y \in X \setminus \{x\}\ y\mu = yv) \Rightarrow \mu \in [\psi]_{\langle A, \cong \rangle}\}$$

where ψ, ψ' are Σ-formulae.

Since all the connectives of the classical first-order logic as well as the existential quantifier can be expressed by means of $\neg$, $\wedge$ and $\forall$, the solutions of an arbitrary first-order logic Σ-formula (without predicate symbols) are well defined by the above definition.

In order to put our formalism in the institution framework we need to investigate the relationship between the solutions across the forgetful functor and the translation of formulae. This is done in the following theorem.

Theorem 8.2. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism and $\langle A', \cong' \rangle$ be an observational Σ'-algebra. For any Σ-formula φ we have*

$$[\varphi]_{\langle A', \cong' \rangle|_\sigma} = ([\sigma(\varphi)]_{\langle A', \cong' \rangle})|_\sigma$$

The proof of this theorem requires the following lemmas.

Lemma 8.3. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism, $\langle A', \cong' \rangle$ be an observational Σ'-algebra and $v \in \mathrm{Val}[X, A'|_\sigma]$ be a valuation. For any Σ-formula ψ we have:*

either $\{v' \in \mathrm{Val}[X', A'] \mid v'|_\sigma = v\} \subseteq [\sigma(\psi)]_{\langle A', \cong' \rangle}$

or $\{v' \in \mathrm{Val}[X', A'] \mid v'|_\sigma = v\} \cap [\sigma(\psi)]_{\langle A', \cong' \rangle} = \emptyset$

Proof. Consider two valuations $v'_1, v'_2 \in \mathrm{Val}[X', A']$ such that $v'_1|_\sigma = v'_2|_\sigma = v$. According to Definition 3.5, v'_1 and v'_2 differ only on values they assign to variables of $X' \setminus \sigma(X)$. This difference cannot have any effect on the fact whether these valuations are solutions of $\sigma(\psi)$, because $\mathrm{Var}[\sigma(\psi)] \subseteq \sigma(X)$. Consequently, either v'_1 and v'_2 are both solutions of $\sigma(\psi)$, or both are not. □

Lemma 8.4. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism and $\langle A', \cong' \rangle$ be an observational Σ'-algebra. For any Σ-formula ψ we have*

$$\mathrm{Val}[X', A']|_\sigma \setminus ([\sigma(\psi)]_{\langle A', \cong' \rangle})|_\sigma = (\mathrm{Val}[X', A'] \setminus [\sigma(\psi)]_{\langle A', \cong' \rangle})|_\sigma$$

Proof. ($\subseteq$) Obvious.

($\supseteq$) Let $v \in (\mathrm{Val}[X', A'] \setminus [\sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma}$. From Lemma 8.3 we have

$$\{v' \in \mathrm{Val}[X', A'] \mid v'_{|\sigma} = v\} \cap [\sigma(\psi)]_{\langle A', \cong' \rangle} = \emptyset$$

Hence $v \notin ([\sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma}$. □

Lemma 8.5. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism, $\langle A', \cong' \rangle$ an observational Σ'-algebra and $v \in \mathrm{Val}[X', A'_{|\sigma}]$ be a valuation. For all Σ-formulae φ, ψ we have*

$$([\sigma(\varphi)]_{\langle A', \cong' \rangle})_{|\sigma} \cap ([\sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma} = ([\sigma(\varphi)]_{\langle A', \cong' \rangle} \cap [\sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma}$$

Proof. ($\subseteq$) Let $v \in ([\sigma(\varphi)]_{\langle A', \cong' \rangle})_{|\sigma} \cap ([\sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma}$. From Lemmas 8.3 and 3.6 we have

$$\{v' \in \mathrm{Val}[X', A'] \mid v'_{|\sigma} = v\} \subseteq [\sigma(\varphi)]_{\langle A', \cong' \rangle}$$

and

$$\{v' \in \mathrm{Val}[X', A'] \mid v'_{|\sigma} = v\} \subseteq [\sigma(\psi)]_{\langle A', \cong' \rangle}$$

Thus

$$\{v' \in \mathrm{Val}[X', A'] \mid v'_{|\sigma} = v\} \subseteq [\sigma(\varphi)]_{\langle A', \cong' \rangle} \cap [\sigma(\psi)]_{\langle A', \cong' \rangle}$$

Hence

$$v \in ([\sigma(\varphi)]_{\langle A', \cong' \rangle} \cap [\sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma}$$

($\supseteq$) Obvious. □

Lemma 8.6. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism, $\langle A', \cong' \rangle$ be an observational Σ'-algebra, x be a variable of X and ψ be a Σ-formula. For any valuation $v' \in \mathrm{Val}[X', A']$ we have:*

$$\forall \mu' \in \mathrm{Val}[X', A'] \quad (\forall y' \in \sigma(X) \setminus \{\sigma(x)\}\ y'\mu' = y'v') \Rightarrow \mu' \in [\sigma(\psi)]_{\langle A', \cong' \rangle} \tag{i}$$

iff

$$\forall \mu' \in \mathrm{Val}[X', A'] \quad (\forall y' \in X' \setminus \{\sigma(x)\}\ y'\mu' = y'v') \Rightarrow \mu' \in [\sigma(\psi)]_{\langle A', \cong' \rangle} \tag{ii}$$

Proof. We use the following notations in the proof:

$$\mathscr{M}_{v'} = \{\mu' \in \mathrm{Val}[X', A'] \mid \forall y' \in \sigma(X) \setminus \{\sigma(x)\}\ y'\mu' = y'v'\}$$

$$\mathscr{P}_{v'} = \{\mu' \in \mathrm{Val}[X', A'] \mid \forall y' \in X' \setminus \{\sigma(x)\}\ y'\mu' = y'v'\}$$

It is obvious that

$$\mathscr{M}_{v'} \subseteq [\sigma(\psi)]_{\langle A', \cong' \rangle} \tag{iii}$$

is equivalent to (i). It is also obvious that

$$\mathscr{P}_{v'} \subseteq [\sigma(\psi)]_{\langle A', \cong' \rangle} \tag{iv}$$

is equivalent to (ii). Consequently, it is enough to prove the equivalence between (iii) and (iv).

(iii) $\Rightarrow$ (iv): Since in $\mathscr{P}_{v'}$ the quantification domain corresponding to $\sigma(X)\setminus\{\sigma(x)\}$ of $\mathscr{M}_{v'}$ is extended to $X'\setminus\{\sigma(x)\}$, we have $\mathscr{P}_{v'} \subseteq \mathscr{M}_{v'}$, hence $\mathscr{P}_{v'} \subseteq [\sigma(\psi)]_{\langle A', \cong' \rangle}$.

(iii) $\Leftarrow$ (iv): Assume $\mu' \in \mathscr{M}_{v'}$ and show that $\mu' \in [\sigma(\psi)]_{\langle A', \cong' \rangle}$. It is clear that there exists $\varrho' \in \mathscr{P}_{v'}$ which coincides with μ' on $\sigma(X)$. Since $\mathrm{Var}[\sigma(\phi)] \subseteq \sigma(X)$, either μ' and ϱ' are solutions of $\sigma(\psi)$ or none of them is. Now, by the hypothesis that ϱ' is a solution of $\sigma(\psi)$, therefore μ' is also $\square$

Lemma 8.7. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism, $\langle A', \cong' \rangle$ be an observational Σ'-algebra, x be a variable of X and ψ be a Σ-formula. For any valuation $v' \in \mathrm{Val}[X', A']$ we have:*

$$\forall \mu' \in \mathrm{Val}[X', A'] \quad (\forall y \in X\setminus\{x\}\ y'\mu'_{|\sigma} = y'v'_{|\sigma}) \Rightarrow \mu'_{|\sigma} \in ([\sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma} \tag{i}$$

iff

$$\forall \mu' \in \mathrm{Val}[X', A'] \quad (\forall y' \in X'\setminus\{\sigma(x)\}\ y'\mu' = y'v') \Rightarrow \mu' \in [\sigma(\psi)]_{\langle A', \cong' \rangle} \tag{ii}$$

Proof. Notice first that the subformula $y'\mu'_{|\sigma} = y'v'_{|\sigma}$ of (i) is equivalent to $\overline{\sigma_{A'}}(y'\mu'_{|\sigma}) = \overline{\sigma_{A'}}(y'v'_{|\sigma})$ since $\overline{\sigma_{A'}}$ is injective, when restricted to the carrier of a given sort. By Definition 3.5 the last equation is equivalent to $\sigma(y)\mu' = \sigma(y)v'$. We can therefore replace the left-hand side of the implication in (i) by $\forall y \in X\setminus\{x\}\ \sigma(y)\mu' = \sigma(y)v'$. Since σ is injective on variables we can change the quantification domain and variable in order to obtain an equivalent formula:

$$\forall y' \in \sigma(X)\setminus\{\sigma(x)\} \quad y'\mu' = y'v' \tag{iii}$$

From Lemma 8.3, we can deduce that the right-hand side of the implication in (i) is equivalent to $\mu' \in [\sigma(\psi)]_{\langle A', \cong' \rangle}$. By substituting it as well as formula (iii) into (i) we obtain the following formula equivalent to (i):

$$\forall \mu' \in \mathrm{Val}[X', A'] \quad (\forall y' \in \sigma(X)\setminus\{\sigma(x)\}\ y'\mu' = y'v') \Rightarrow \mu' \in [\sigma(\psi)]_{\langle A', \cong' \rangle}$$

By Lemma 8.6 this last formula is equivalent to (ii). $\square$

Proof of Theorem 8.2. By structural induction on a Σ-formula φ under the induction hypothesis that the theorem holds for all proper subformula of φ.

Base step: φ is an equation $l = r$. We have to consider two cases:

Case 1: There exists a sort $s \in S$ such that $A'_{\sigma(s)} = \emptyset$ and $x_s \in \mathrm{Var}[l, r]$. By Definition 8.1 we have

$$[l = r]_{\langle A, \cong \rangle_{|\sigma}} = \mathrm{Val}[X, A'_{|\sigma}]$$

$$[\sigma(l) = \sigma(r)]_{\langle A', \cong' \rangle} = \mathrm{Val}[X', A']$$

By Lemma 3.6 we know that $-_{|\sigma}$ is total and surjective on valuations, consequently

$$\mathrm{Val}[X', A']_{|\sigma} = \mathrm{Val}[X, A'_{|\sigma}]$$

Hence $([\sigma(l=r)]_{\langle A', \cong'\rangle})_{|\sigma} = [l=r]_{\langle A, \cong\rangle_{|\sigma}}$.

Case 2: Neither l nor r contains a variable of sort s such that $A'_{\sigma(s)} = \emptyset$. From Definition 8.1 we have $v \in [l=r]_{\langle A', \cong'\rangle_{|\sigma}}$ if and only if $v: X \to A'_{|\sigma}$ and

$$\overline{lv} \cong'_{|\sigma} \overline{rv} \tag{iv}$$

From Lemma 3.6 we know that any $v: X \to A'_{|\sigma}$ has the form $v'_{|\sigma}$ with $v': X' \to A'$ and that $\mu'_{|\sigma}$ exists for any $\mu': X' \to A'$. So (iv) is equivalent to $\overline{lv'_{|\sigma}} \cong'_{|\sigma} \overline{rv'_{|\sigma}}$, by Definition 7.4 is equivalent to $\overline{\sigma_{A'}}(\overline{lv'_{|\sigma}}) \cong' \overline{\sigma_{A'}}(\overline{rv'_{|\sigma}})$ and by Lemma 3.7 is equivalent to $\overline{\sigma(l)v'} \cong' \overline{\sigma(r)v'}$. This last formula holds if and only if $v' \in [\sigma(l) = \sigma(r)]_{\langle A', \cong'\rangle}$.

Induction step:

- $\varphi = \neg\psi$

$$\begin{aligned}
[\neg\psi]_{\langle A, \cong\rangle_{|\sigma}} &= \mathrm{Val}[X, A'_{|\sigma}] \setminus [\psi]_{\langle A', \cong'\rangle_{|\sigma}} && \text{(by the induction hypothesis)}\\
&= \mathrm{Val}[X, A'_{|\sigma}] \setminus ([\sigma(\psi)]_{\langle A', \cong'\rangle})_{|\sigma} && \text{(by the injectivity of } -_{|\sigma})\\
&= \mathrm{Val}[X', A'])_{|\sigma} \setminus ([\sigma(\psi)]_{\langle A', \cong'\rangle})_{|\sigma} && \text{(by Lemma 8.4)}\\
&= (\mathrm{Val}[X', A'] \setminus ([\sigma(\psi)]_{\langle A', \cong'\rangle})_{|\sigma} && \text{(by Definition 8.1)}\\
&= ([\neg\sigma(\psi)]_{\langle A', \cong'\rangle})_{|\sigma}\\
&= ([\sigma(\neg\psi)]_{\langle A', \cong'\rangle})_{|\sigma}
\end{aligned}$$

- $\varphi = \psi_1 \wedge \psi_2$

$$\begin{aligned}
[\psi_1 \wedge \psi_2]_{\langle A', \cong'\rangle_{|\sigma}} &= [\psi_1]_{\langle A', \cong'\rangle_{|\sigma}} \cap [\psi_2]_{\langle A', \cong'\rangle_{|\sigma}} && \text{(by the induction hypothesis)}\\
&= ([\sigma(\psi_1)]_{\langle A', \cong'\rangle})_{|\sigma} \cap ([\sigma(\psi_2)]_{\langle A', \cong'\rangle})_{|\sigma} && \text{(by Lemma 8.4)}\\
&= ([\sigma(\psi_1)]_{\langle A', \cong'\rangle} \cap [\sigma(\psi_2)]_{\langle A', \cong'\rangle})_{|\sigma} && \text{(by Definition 8.1)}\\
&= ([\sigma(\psi_1) \wedge \sigma(\psi_2)]_{\langle A', \cong'\rangle})_{|\sigma}\\
&= ([\sigma(\psi_1 \wedge \psi_2)]_{\langle A', \cong'\rangle})_{|\sigma}
\end{aligned}$$

- $\varphi = \forall x\, \psi$

$$\begin{aligned}
[\forall x\, \psi]_{\langle A', \cong'\rangle} = \{ & v \in \mathrm{Val}[X, A'_{|\sigma}] \mid \forall \mu \in \mathrm{Val}[X, A'_{|\sigma}]\ (\forall y \in X \setminus \{x\}\ y\mu = yv)\\
& \Rightarrow \mu \in [\psi]_{\langle A, \cong\rangle} \} && \text{(by the induction hypothesis)}\\
= \{ & v \in \mathrm{Val}[X, A'_{|\sigma}] \mid \forall \mu \in \mathrm{Val}[X, A'_{|\sigma}]\ (\forall y \in X \setminus \{x\}\ y\mu = yv)\\
& \Rightarrow \mu \in ([\sigma(\psi)]_{\langle A, \cong\rangle})_{|\sigma} \} && \text{(by injectivity of } -_{|\sigma} \text{ on valuations)}
\end{aligned}$$

$$= \{v' \in \mathrm{Val}[X, A'] \mid \forall \mu' \in \mathrm{Val}[X', A'] \ (\forall y \in X \setminus \{x\} \ y'\mu'_{|\sigma} = y'v'_{|\sigma})$$

$$\Rightarrow \mu'_{|\sigma} \in ([\sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma}\}_{|\sigma} \quad \text{(by Lemma 8.7)}$$

$$= \{v' \in \mathrm{Val}[X, A'] \mid \forall \mu' \in \mathrm{Val}[X', A'] \ (\forall y' \in X' \setminus \{\sigma(x)\} \ y'\mu' = y'v'$$

$$\Rightarrow \mu' \in [\sigma(\psi)]_{\langle A', \cong' \rangle}\}_{|\sigma} \quad \text{(by Definition 8.1)}$$

$$= ([\forall \sigma(x) \sigma(\psi)]_{\langle A', \cong' \rangle})_{|\sigma} = ([\sigma(\forall x \psi)]_{\langle A', \cong' \rangle})_{|\sigma} \qquad \square$$

Definition 8.8. An **observational Σ-sentence** is a pair $\langle \varphi, W \rangle$ where $\varphi \in \mathrm{Wfs}[\Sigma]$ is a Σ-sentence and $W \subseteq T_\Sigma(X)$ is a set of terms. We note **OWfs[Σ]** the set of all observational Σ-sentences.

As in the usual framework, OWfs is extended to a functor from the category of signatures Sig to Set (the category of sets). This functor maps every object Σ of Sig to the set of all observational Σ-sentences. An arrow σ of $\mathrm{Sig}(\Sigma, \Sigma')$ is mapped by OWfs to the product map of its usual extensions on $\mathrm{Wfs}[\Sigma]$ and $T_\Sigma(X)$. In other words,

$$\mathrm{OWfs}[\sigma](\langle \varphi, W \rangle) = \langle \sigma(\varphi), \sigma(W) \rangle$$

(We write ambiguously σ instead of $\mathrm{OWfs}[\sigma]$.)

We have already all the elements necessary to define an observational satisfaction relation.

Definition 8.9. We say that an observational Σ-algebra $\langle A, \cong \rangle$ **satisfies** an observational sentence $\langle \psi, W \rangle$, written $\langle A, \cong \rangle \not\models (\psi, W)$, iff

$$[\psi]_{\langle A, \cong \rangle} = \mathrm{Val}[X, A] \tag{i}$$

$$\cong \subseteq \sim_W \tag{ii}$$

Notice that in the above we have defined a family of relations $\{\not\models_\Sigma\}_{\Sigma : \mathrm{Sig}}$ with

$$\not\models_\Sigma \subseteq \mathrm{OAlg}[\Sigma] \times \mathrm{OWfs}[\Sigma]$$

We examine now how our satisfaction relation behaves w.r.t. the variance of observational sentences (translation) and the covariance of algebras (σ-reduct). We start by the first requirement of Definition 8.9.

Proposition 8.10. *Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. For any set of terms $W \subseteq T_\Sigma(X)$, any observational Σ'-algebra $\langle A', \cong' \rangle$ and any Σ-formula φ we have*

$$[\sigma(\varphi)]_{\langle A', \cong' \rangle} = \mathrm{Val}[X', A'] \quad \textit{iff} \quad [\varphi]_{\langle A', \cong' \rangle_{|\sigma}} = \mathrm{Val}[X, A'_{|\sigma}]$$

Proof. We have $[\sigma(\varphi)]_{\langle A', \cong' \rangle} = \mathrm{Val}[X', A']$ equivalent to $([\sigma(\varphi)]_{\langle A', \cong' \rangle})_{|\sigma} = (\mathrm{Val}[X', A'])_{|\sigma}$, which by Theorem 8.2 is equivalent to

$$[\varphi]_{\langle A', \cong' \rangle_{|\sigma}} = (\mathrm{Val}[X', A'])_{|\sigma} \quad \text{(i)}$$

According to Lemma 3.6, $-_{|\sigma}$ is surjective on the valuations. Consequently, we have $(\mathrm{Val}[X', A'])_{|\sigma} = \mathrm{Val}[X, A'_{|\sigma}]$. Thus, the formula (i) is equivalent to $[\varphi]_{\langle A', \cong' \rangle_{|\sigma}} = \mathrm{Val}[X, A'_{|\sigma}]$. □

The next step is to study the second condition of Definition 8.9 w.r.t. term translation and forgetful functor. We examine first the if part and then the converse part of this condition.

Proposition 8.11. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism. For all sets of terms $W \subseteq T_\Sigma(X)$, $W' \subseteq T_{\Sigma'}(X')$ such that $\sigma(W) \subseteq W'$ and for any observational Σ'-algebra $\langle A', \cong' \rangle$ we have*

$$\cong' \subseteq \sim_{W'} \Rightarrow \cong'_{|\sigma} \subseteq \sim_W$$

where $\sim_{W'}$ and $\sim_W$ are the indistinguishability relations on A' and $A'_{|\sigma}$ respectively.

Proof. Assume that

$$\forall a', b' \in A' \quad a' \cong' b' \Rightarrow a' \sim_{W'} b' \quad \text{(i)}$$

This holds particularly for $a', b' \in A'_{\sigma(s)}$ (for some $s \in S$). Since $\overline{\sigma_{A'}}: A'_{|\sigma} \to A'$ with range $\coprod_{s \in S} A'_{\sigma(s)}$, from (i) we deduce that

$$\forall a, b \in A'_{|\sigma} \quad \overline{\sigma_{A'}}(a) \cong' \overline{\sigma_{A'}}(b) \Rightarrow \overline{\sigma_{A'}}(a) \sim_{W'} \overline{\sigma_{A'}}(b)$$

By Definition 7.4, $\overline{\sigma_{A'}}(a) \cong' \overline{\sigma_{A'}}(b)$ is equivalent to $a \cong'_{|\sigma} b$. Hence

$$\forall a, b \in A'_{|\sigma} \quad a \cong'_{|\sigma} b \Rightarrow \overline{\sigma_{A'}}(a) \sim_{W'} \overline{\sigma_{A'}}(b)$$

But from Proposition 5.1 it follows that $\overline{\sigma_{A'}}(a) \sim_{W'} \overline{\sigma_{A'}}(b) \Rightarrow a \sim_W b$. Consequently

$$\forall a, b \in A'_{|\sigma} \quad a \cong'_{|\sigma} b \Rightarrow a \sim_{W'} b. \qquad \square$$

The next step should be to prove the converse of the above proposition restricted to $W' = \sigma(W)$. Unfortunately this is not true in general. The following example illustrates this fact.

Example 8.12. Consider the following signatures:

$$\Sigma = \{ \quad a, b : \to s \quad \text{true, false} : \to \mathrm{Bool} \quad f, g : s \to \mathrm{Bool} \ \}$$

$$\Sigma' = \{ \quad c, d : \to s \quad \text{true, false} : \to \mathrm{Bool} \quad h : s \to \mathrm{Bool} \ \}$$

Let $W=\{f(a), g(b)\}$. Notice that in any Σ-algebra A we have

$$a^A \sim_W b^A \tag{i}$$

because a^A and b^A have no comparator. Consider $\sigma: \Sigma \to \Sigma'$ defined by:

$$\sigma(\text{Bool})=\text{Bool} \quad \sigma(\text{true})=\text{true} \quad \sigma(a)=c$$

$$\sigma(s)=s \qquad \sigma(\text{false})=\text{false} \quad \sigma(b)=d$$

$$\sigma(f)=\sigma(g)=h$$

Notice that in any Σ'-algebra A',

$$\text{cmp}_{\sigma(W)}(c^{A'}, d^{A'})=(h(\diamond)\} \tag{ii}$$

since $\sigma(W)=\{h(c), h(d)\}$.

Consider a reachable observational Σ'-algebra $\langle A', \cong' \rangle$ such that

$$h^{A'}(c^{A'}) \neq h^{A'}(d^{A'}) \tag{iii}$$

$$c^{A'} \cong' d^{A'} \tag{iv}$$

Notice that $\cong'_{|\sigma}=\{a^{A_{|\sigma}}, b^{A_{|\sigma}})\}$. Therefore, according to (i) we have

$$\cong'_{|\sigma} \subseteq \sim_W$$

but we have not $\cong' \subseteq \sim_{\sigma(W)}$ since from (ii) and (iii) we have $c^{A'} \not\sim_{\sigma(W)} d^{A'}$ whereas from (iv) we have $c^{A'} \cong' d^{A'}$.

From this negative result we may already conclude that, in order to establish institutions within our approach, we will be constrained to restrict our framework somehow. This will be the subject of Section 10.

9. Observational specifications

This section is devoted to some general notions about observational specifications.

Definition 9.1. An **observational specification** OSP is a tuple $\langle \Sigma, \Theta, W \rangle$, where Σ is the signature of OSP, Θ the set of its axioms and W is a set of terms with variables, $W \subseteq T_\Sigma(X)$, called **observations** of OSP.

The models are defined as in the usual approach except that we use the observational satisfaction instead of the usual one.

Definition 9.2. Let $\mathrm{OSP}=\langle \Sigma, \Theta, \mathrm{W}\rangle$ be an observational specification. We say that an observational Σ-algebra $\langle A, \cong\rangle$ is a **model** of OSP iff

$$\forall \theta \in \Theta \quad \langle A, \cong\rangle \not\models \langle \theta, \mathrm{W}\rangle$$

We note **OAlg[OSP]** the class of all observational models of OSP.

In the above definition we have considered a set $\Phi=\{\varphi_1, \ldots, \varphi_n\}$ of formulae as a conjunction of formulae $\Phi=\varphi_1 \wedge \cdots \wedge \varphi_n$. Thus any pair $\langle \Phi, \mathrm{W}\rangle$ can be viewed as a single observational sentence. One may also define an observational specification as a pair $\langle \Sigma, \mathrm{OAx}\rangle$ with $\mathrm{OAx}=\{\langle \theta_1, \mathrm{W}_1\rangle, \ldots, \{\langle \theta_i, \mathrm{W}_i\rangle, \ldots\}$. The possibility to associate observations separately to each axiom would increase the expressive power. However, in all examples it seems preferable to attach a unique set of observation terms to the whole specification.

Fact 9.3. *The observational algebra* $\langle L_{|\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}}\rangle$, *described in Example* 7.2, *is a model of the observational specification* SWE.

Proof. Since the observational equality on $\langle L_{|\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}}\rangle$ is just the indistinguishability relation, we only need to prove that for any axiom θ of SWE we have

$$[\theta]_{\langle L_{|\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}}\rangle}=\mathrm{Val}[\mathrm{X}, L_{|\sigma}]$$

Notice that $(L_{|\sigma})_{|\mathsf{Sig[LIST]}}=L$. On the other hand from Example 4.7 we know that $\sim_{\mathrm{Obs}_{\mathsf{SWE}}}$ is the usual equality on $(L_{|\sigma})_{|\mathsf{Sig[LIST]}}$. We have therefore

$$(\langle L_{|\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}}\rangle)_{|\mathsf{Sig[LIST]}}=\langle L, =\rangle$$

and since L is a model of LIST, $\langle L_{|\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}}\rangle$ satisfies all the axioms of LIST.

Since the elements observationally equal on $(L_{|\sigma})_{\mathsf{Set}}$ are different representations of the same set, it is clear that for the "standard" axioms $\psi_1, \psi_2, \ldots, \psi_8$ of sets (see Fig. 1), we have

$$[\psi_i]_{\langle L_{|\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}}\rangle}=\mathrm{Val}[\mathrm{X}, L_{|\sigma}]$$

Notice that ψ_9 and ψ_{10} are translated by σ (see Example 4.7) in the following way:

$\sigma(\psi_9)$: $\mathsf{idl(nil)=nil}$

$\sigma(\psi_{10})$: $\mathsf{idl(cons(x, l))=cons(x, idl(l))}$

We have therefore

$$[\sigma(\psi_9)]_{\langle L, =\rangle}=[\sigma(\psi_{10})]_{\langle L, =\rangle}=\mathrm{Val}[\mathrm{X}, L]$$

Then, according to Theorem 8.2, we obtain

$$[\psi_9]_{\langle L_{|\sigma}, =\rangle}=[\psi_{10}]_{\langle L_{|\sigma}, =\rangle}=\mathrm{Val}[\mathrm{X}, L_{|\sigma}]$$

Hence we can conclude that

$$[\psi_9]_{\langle L_{|\sigma},\ \sim_{\mathrm{Obs}_{\mathrm{SWE}}}\rangle} = \langle \psi_{10} \rangle_{\langle L_{|\sigma},\ \sim_{\mathrm{Obs}_{\mathrm{SWE}}}\rangle} = \mathrm{Val}[\mathrm{X}, L_{|\sigma}]$$

The last step is justified by the fact that the axioms ψ_9 and ψ_{10} are equations and that $= \subseteq \sim_{\mathrm{Obs}_{\mathrm{SWE}}}$. Obviously, for any Σ-equation $t = t'$, any Σ-algebra A and the observational equalities $\cong^{\alpha} \subseteq \cong^{\beta}$ on A, we have $[t = t']_{\langle A, \cong^{\alpha}\rangle} \subseteq [t = t']_{\langle A, \cong^{\beta}\rangle}$. □

In the above example we have considered a model of the form $\langle A, \sim_{\mathrm{W}}\rangle$. Of course, this is possible only when $\sim_{\mathrm{W}}$ is transitive. Moreover this model has a particular status: it is a terminal object in the category of all observational models formed with a given algebra A. (This is quite analogous to the final data type of [12].) Notice that when $\sim_{\mathrm{W}}$ is not transitive this category has often no terminal object. For instance the category of observational models of TRANS formed with the algebra A (see Fig. 2) has no terminal object.

The next result points out that our observational specifications together with their semantics generalize the usual approach. On the one hand an algebra A can be viewed as the observational algebra $\langle A, = \rangle$. On the other hand, an algebraic specification $\langle \Sigma, \Theta \rangle$ can be considered as an observational one in the straightforward way: we just take $\langle \Sigma, \Theta, \mathrm{X} \rangle$. The relationship between the two is stated by the following proposition.

Proposition 9.4. *Let $\langle \Sigma, \Theta \rangle$ be an algebraic specification. Each model of $\langle \Sigma, \Theta, \mathrm{X} \rangle$ is of the form $\langle A, = \rangle$ with $A \in \mathrm{Alg}[\langle \Sigma, \Theta \rangle]$.*

Proof. Notice first that $\sim_{\mathrm{X}}$ is the identity relation on any Σ-algebra. This is obvious since a variable $x \in \mathrm{X}_s$ gives rise to an empty comparator $\diamond_s$ which distinguishes all distinct $a, b \in A_s$ and we have assumed that X_s is nonempty for any sort s. By Definition 8.9, for any $\langle A, \cong \rangle \in \mathrm{OAlg}[\langle \Sigma, \Theta, \mathrm{X} \rangle]$ we have $\cong \subseteq \sim_{\mathrm{X}}$, thus $\cong$ is just the usual equality. From the requirement $[\theta]_{\langle A, = \rangle} = \mathrm{Val}[\mathrm{X}, A]$, for all $\theta \in \Theta$, we deduce that $A \in \mathrm{Alg}[\langle \Sigma, \Theta \rangle]$. Conversely, it is clear that for any $B \in \mathrm{Alg}[\langle \Sigma, \Theta \rangle]$ we have $\langle B, = \rangle \in \mathrm{OAlg}\langle \Sigma, \Theta, \mathrm{X} \rangle]$. □

Up to now, we have not been studying modularity issues. We have only defined the semantics of "flat" specifications. In fact, as in [1], our semantics extends to an observational stratified loose semantics without additional assumptions. For instance, the next theorem shows that our approach fulfils the requirement of "reusing by restriction" [3].

Theorem 9.5. *Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. For all observational specifications $\mathrm{OSP} = \langle \Sigma, \Theta, \mathrm{W} \rangle$ and $\mathrm{OSP}' = \langle \Sigma', \Theta', \mathrm{W}' \rangle$ such that $\sigma(\Theta) \subseteq \Theta'$ and $\sigma(\mathrm{W}) \subseteq \mathrm{W}'$ we have*

$$\mathrm{OAlg}[\mathrm{OSP}']_{|\sigma} \subseteq \mathrm{OAlg}[\mathrm{OSP}].$$

Proof. From Definitions 9.2 and 8.9 it is enough to prove

$$\forall \langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$$

$$(\forall \theta' \in \Theta' \ [\theta']_{\langle A', \cong' \rangle} = \mathrm{Val}[\mathrm{X}', A'] \Rightarrow (\forall \theta \in \Theta \ [\theta]_{\langle A', \cong' \rangle|_\sigma} = \mathrm{Val}[\mathrm{X}, A'|_\sigma]) \qquad \text{(i)}$$

and

$$\forall \langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma'] \quad \cong' \subseteq \sim_{\mathbf{W}'} \Rightarrow \cong'|_\sigma \subseteq \sim_{\mathbf{W}} \qquad \text{(ii)}$$

Proof of (i): Let $\langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$ such that

$$\forall \theta' \in \Theta' \quad [\theta']_{\langle A', \cong' \rangle} = \mathrm{Val}[\mathrm{X}', A']$$

Since $\sigma(\Theta) \subseteq \Theta'$, for all $\theta \in \Theta$ we have $[\sigma(\theta)]_{\langle A', \cong' \rangle} = \mathrm{Val}[\mathrm{X}', A']$. According to Proposition 8.10

$$\forall \theta \in \Theta \quad [\theta]_{\langle A', \cong' \rangle|_\sigma} = \mathrm{Val}[\mathrm{X}', A'|_\sigma]$$

Proof of (ii) follows directly from Proposition 8.11. □

This result corresponds to a very fundamental property which holds in most nonobservational frameworks. *Except for our case, in all other approaches with an observational satisfaction relation the corresponding property holds only for equational specifications.* It may also hold for positive-conditional axioms under the hypothesis of observable premises. However, this is a rather strong restriction. It may be then surprising that in our approach the former theorem holds without restriction even if the axioms are arbitrary first-order sentences. The reason is that our observational equality is not fixed by observations contrary to the indistinguishability relation. Unlike [1, 23, 8, 16, 19][7] our observational equality does not coincide with the indistinguishability relation. This choice was dictated by the fact that the indistinguishability relation is "disconnected" from the forgetful functor. On the contrary, our observational equality, similarly to the usual equality, is always "transported" through the forgetful functor. The main difference of our approach with the above-mentioned works is that our satisfaction relation is based on an observational equality which does not coincide with the indistinguishability relation. This situation (party) guarantees such a general result as Theorem 9.5.

The following corollary of the former theorem formalizes the phenomenon: "more observations, less models".

[7] Even if observational equality is not explicitly defined in all these approaches, it is indeed straightforward to define it, as shown in [14].

Corollary 9.6. *Let* $\mathrm{OSP}_1 = \langle \Sigma, \Theta, \mathrm{W}_1 \rangle$ *and* $\mathrm{OSP}_2 = \langle \Sigma, \Theta, \mathrm{W}_2 \rangle$ *be observational specifications such that* $\mathrm{W}_1 \subseteq \mathrm{W}_2$. *Then*

$$\mathrm{OAlg}[\mathrm{OSP}_2] \subseteq \mathrm{OAlg}[\mathrm{OSP}_1]$$

Proof. Follows directly from the previous theorem. □

We conclude from the above that observations act on the semantics of a specification in a quite similar way as the axioms, since by adding axioms, we restrict the class of the models.

10. Towards an institution of observational specifications

In this section, based on the framework we have developed so far, we define an institution for observational specifications. As mentioned in Section 8, this task requires some additional restrictions.

Recall that an institution (see [7]) is a tuple $\langle$Sign, Wfs, Mod, $\models\rangle$ where

1. Sign is a category of "signatures",
2. $\mathrm{Wfs}: \mathrm{Sign} \to \mathrm{Set}$ is a functor which maps each signature to the set of well-formed sentences over the signature, and each signature morphism to its extension on sentences (translation map),
3. $\mathrm{Mod}: \mathrm{Sign} \to \mathrm{Cat}^{\mathrm{op}}$ is a functor which maps a signature to the category of the interpretation structures (models), and each signature morphism to the σ-reduct functor $(-_{|\sigma}: \mathrm{Mod}[\Sigma'] \to \mathrm{Mod}[\Sigma])$,
4. $\models$ is a ($|\mathrm{Sign}|$-sorted) satisfaction relation ($\models_\Sigma \subseteq \mathrm{Mod}[\Sigma] \times \mathrm{Wfs}[\Sigma]$) such that for each $\sigma: \Sigma \to \Sigma'$ in Sign, each $\varphi \in \mathrm{Wfs}[\Sigma]$ and each $M' \in \mathrm{Mod}[\Sigma']$ the following **satisfaction condition** holds:

$$M' \models \mathrm{Wfs}[\sigma](\varphi) \quad \text{iff } \mathrm{Mod}[\sigma](M') \models \varphi$$

It is clear that the tuple $\langle$Sig, OWfs, OAlg, $\not\models\rangle$ could be an institution provided that it would fulfil the satisfaction condition which in our formalism is expressed by the following property.

Property 10.1. *For any* $\sigma: \Sigma \to \Sigma'$, *any observational* Σ*-sentence* $\langle \varphi, \mathrm{W} \rangle$ *and any observational* Σ'*-algebra*

$$\langle A', \cong' \rangle \not\models \sigma(\langle \varphi, \mathrm{W} \rangle) \quad \textit{iff } \langle A', \cong' \rangle_{|\sigma} \not\models \langle \varphi, \mathrm{W} \rangle$$

By Definition 8.9 in order to show that this property holds, it is enough to prove

$$\forall \langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$$

$$[\sigma(\varphi)]_{\langle A', \cong' \rangle} = \mathrm{Val}[\mathrm{X}', A'] \Leftrightarrow [\varphi]_{\langle A', \cong' \rangle_{|\sigma}} = \mathrm{Val}[\mathrm{X}, A'_{|\sigma}] \qquad \text{(i)}$$

and

$$\forall \langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma'] \quad \cong' \subseteq \sim_{\sigma(W)} \Leftrightarrow \cong'_{|\sigma} \subseteq \sim_W \tag{ii}$$

The first requirement is guaranteed by Proposition 8.10. From Proposition 8.11 we have the "only if" condition of the second requirement. Unfortunately, we know from Example 8.12 that its converse part does not hold without additional assumptions. The following is the necessary and sufficient condition of the converse part of (ii).

Property 10.2. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism and $W \subseteq T_\Sigma(X)$ be a set of terms. For all Σ'-algebras A' and all $\sigma(W)$-distinguishable $a', b' \in A'_{\sigma(s)}$, there exist $a, b \in (A'_{|\sigma})_s$ satisfying $\overline{\sigma_{A'}}(a) = a'$ and $\overline{\sigma_{A'}}(b) = b'$ such that*

$$a \not\sim_W b$$

Proposition 10.3. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism. Property* 10.2 *holds for a set W of Σ-terms if and only if*

$$\cong'_{|\sigma} \subseteq \sim_W \Rightarrow \cong' \subseteq \sim_{\sigma(W)}$$

holds on all $\langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$.

Proof. ($\Rightarrow$) Let $\langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$. Assume that

$$\forall a, b \in A'_{|\sigma} \quad a \cong'_{|\sigma} b \Rightarrow a \sim_W b \tag{i}$$

By contradiction assume that there exist $a_1, b_1 \in A'_{|\sigma}$ such that

$$\overline{\sigma_{A'}}(a_1) \not\sim_{\sigma(W)} \overline{\sigma_{A'}}(b_1) \tag{ii}$$

$$\overline{\sigma_{A'}}(a_1) \cong' \overline{\sigma_{A'}}(b_1) \tag{iii}$$

Using Property 10.2, from (ii) we deduce that there exist $a_2, b_2 \in A'_{|\sigma}$ such that

$$\overline{\sigma_{A'}}(a_2) = \overline{\sigma_{A'}}(a_1) \tag{iv}$$

$$\overline{\sigma_{A'}}(b_2) = \overline{\sigma_{A'}}(b_1) \tag{v}$$

$$a_2 \not\sim_W b_2 \tag{vi}$$

But according to (iii), (iv) and (v) we conclude that $a_2 \cong'_{|\sigma} b_2$. We have therefore

$$a_2 \cong'_{|\sigma} b_2 \not\Rightarrow a_2 \sim_W b_2$$

which is in contradiction with the assumption (i).

($\Leftarrow$) (We prove it in an indirect way.) Let $\sigma: \Sigma \to \Sigma'$ and $W \subseteq T_\Sigma(X)$ for which Property 10.2 does not hold. Consequently, there is a Σ'-algebra A' with elements

$a', b' \in A'_{\sigma(s_0)}$ (for some $s_0 \in S$) $\sigma(W)$-distinguishable, such that for any $s \in S$ satisfying $\sigma(s) = \sigma(s_0)$, all the elements $a, b \in (A'|_\sigma)_s$ such that $\overline{\sigma_{A'}}(a) = a'$ and $\overline{\sigma_{A'}}(b) = b'$ are W-indistinguishable. Equip A' with $\cong'$ such that $c' \cong' d' \Rightarrow c' \sim_{\sigma(W)} d'$ for all $c', d' \in A'$ except for a', b' where $a' \cong' b'$. It is clear from the proof of Proposition 8.11 that for all these c', d' we have also that for all the elements $c, d \in (A'|_\sigma)_s$ such that $\overline{\sigma_{A'}}(c) = c'$ and $\overline{\sigma_{A'}}(d) = d'$ the following holds:

$$c \cong'|_\sigma d \Rightarrow c \sim_W d.$$

It follows from the above formula that $\cong'|_\sigma \subseteq \sim_W$, since by Definition 7.4 we have $a \cong'|_\sigma b$ and we have assumed that $a \sim_W b$. Now, $\cong' \not\subseteq \sim_{\sigma(W)}$ because $a' \cong' b'$ and we have assumed that $a' \not\sim_{\sigma(W)} b'$. □

We can conclude from the above that in our approach, the satisfaction condition does not hold in general. Only the "only if" part of Property 10.1 holds. Consequently, according to [20], our approach defines a reduction-preserving-satisfaction pre-institution. The converse part of Property 10.1 holds only for those signature morphisms and those observations which enjoy Property 10.2. Consequently our approach could motivate more liberal formalizations of the notion of "logical system" than institutions, as e.g. specification logics [4] or pre-institutions [20]. One of such formalizations could be **partial institutions** where translation of sentences is partial and satisfaction condition is required only for translatable sentences. In our case an observational Σ-formula $\langle \varphi, W \rangle$ would be defined as translatable w.r.t $\sigma: \Sigma \to \Sigma'$ iff $\sigma^{-1}(\sigma(W)) = W$. This is justified by the following corollary.

Corollary 10.4. *Let $\sigma: \Sigma \to \Sigma'$ be a signature morphism and $W \subseteq T_\Sigma(X)$ be a set of terms such that $\sigma^{-1}(\sigma(W)) = W$. Then σ and W satisfy Property 10.2.*

Proof. Obvious from Proposition 5.2. □

Since the satisfaction condition holds only for some signature morphisms, in order to define an institution in our framework, one could forget some problematic arrows of Sig and consider as a category of signatures a category which has the same objects as Sig but less arrows. We retain this last solution. Then the question is which signature morphisms we should eliminate in order to obtain an institution. Thanks to Corollary 10.4 we notice that problematic arrows are those which do not preserve

$$\forall W \subseteq T_\Sigma(X) \quad \sigma^{-1}(\sigma(W)) = W$$

It is easy to see that the above equation is satisfied by any signature morphism for which the corresponding map on operations (and not necessarily on sorts) is injective. This remark leads to the following result.

Proposition 10.5. *Consider the tuple* $\mathrm{OAlgSpec} = \langle \mathrm{ISig}, \mathrm{OWfs}, \mathrm{OAlg}, \not\models \rangle$ *where* ISig *is the category whose objects are the usual signatures and whose arrows are all signature morphisms for which the corresponding maps on operations are injective. Then* OAlgSpec *is an institution.*

Proof. Follows from the above comment. □

Notice that OAlgSpec denotes in fact a family of institutions. Recall that

$$\mathrm{OWfs}[\Sigma] = \{\langle \varphi, \mathrm{W} \rangle \mid \varphi \in \mathrm{Wfs}[\Sigma],\ \mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})\}$$

Accordingly, OAlgSpec is in some sense "parametrized" by Wfs. Recall that our approach does not take into account predicate symbols (other than $=$). Thus the Wfs functors acceptable for our purposes must send every signature to any appropriate subset of the corresponding language of many-sorted first-order logic with equality but without predicate symbols. Moreover, our approach can be easily enriched with predicate symbols without loss of results (as shown in [13]).

11. Some additional examples

In this section we show on two examples how some (usual) algebraic specification $\langle \Sigma, \Theta \rangle$ can be completed with observations W, in order to get some interesting observational models corresponding to bounded realizations. Of course the examples of models we provide are only in $\mathrm{OAlg}[\langle \Sigma, \Theta, \mathrm{W} \rangle]$ and not in $\mathrm{Alg}[\langle \Sigma, \Theta \rangle]$. This motivates the use of an observational approach to handle bounded implementations of specifications which (in the usual sense) have no bounded models. In both examples we proceed as follows:

1. Given a specification $\langle \Sigma, \Theta \rangle$ we provide a Σ-algebra A which is not a model of $\langle \Sigma, \Theta \rangle$.
2. We equip A with an observational equivalence $\cong$ and we show that $\langle A, \cong \rangle$ fulfils the first requirement of the definition of our observational satisfaction relation 8.9, that is $[\theta]_{\langle A, \cong \rangle} = \mathrm{Val}[\mathrm{X}, A]$ for all $\theta \in \Theta$.
3. We give an appropriate set of observations W and we show that the second requirement of the definition of our satisfaction relation holds, that is $\cong \subseteq \sim_{\mathrm{W}}$.

As a first example consider the specification $\mathsf{INT} = (\langle \Sigma_1, \Theta_1 \rangle$ of integers (see Fig. 3). The only reachable models of this specification are $\mathbb{Z}$ and all the $\mathbb{Z}/n\mathbb{Z}$. Assume that we need a realization of this specification which behaves like $\mathbb{Z}$ at least inside an interval between the constants minint and maxint. Consider the Sig[INT]-algebra A in Fig. 4. Obviously, this algebra is not a model of INT.

Let us equip A with the observational equality "$\cong$" defined as the reflexive-symmetric-transitive closure of the relation

$$\{\langle \mathit{minint}, \mathit{underflow} \rangle, \langle \mathit{maxint}, \mathit{overflow} \rangle\}$$

spec: INT	**spec:** STACK
sort: Int	**use:** NAT
operations:	**sort:** Stack
0 : Int	**operations:**
s, p : Int→Int	emptystack : →Stack
axioms:	push : Nat Stack→Stack
p(s(x)) = x	top : Stack→Nat
s(p(x)) = x	pop : Stack→Stack
	axioms:
	top(push(x, s)) = x
	pop(push(x, s)) = s

Fig. 3. Specifications INT and STACK.

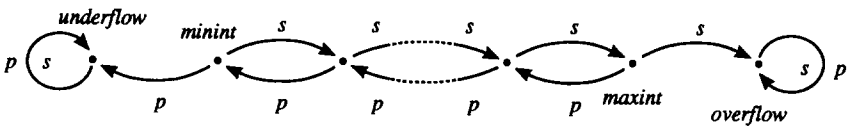

Fig. 4.

It is easy to show that Val[X, A] is the set of solutions of both axioms of INT in $\langle A, \cong \rangle$. Assume now that we observe the set W_1 of all the ground terms which denote integers between minint and maxint. In this situation the contextual variable $\diamond_{\text{Int}}$ is an observable context of all the elements of A between *minint* and *maxint*. On the contrary, *underflow* and *overflow* have no observable context. Consequently

$$\sim_{W_1} = \{\langle b, b\rangle, \langle c, d\rangle \mid b, c, d \in A_{\text{Int}},\ \{c, d\} \cap \{\textit{underflow}, \textit{overflow}\} \neq \emptyset\}$$

Hence $\cong \subseteq \sim_{W_1}$ and we conclude that $\langle A, \cong \rangle$ is an observational model of $\langle \Sigma_1, \Theta_1, W_1 \rangle$.

As a second example, we are going to study bounded stacks. Consider the specification STACK $= (\Sigma_2, \Theta_2\rangle$ (see Fig. 3) and assume that we are only interested in stacks of a height bounded by a constant *maxheight*. Then the following algebra A should be correct for our purposes: we consider an array-pointer realization with an array of length *maxheight* + 1 starting at the index 0. A full stack is then represented by the couple $\langle t, \textit{maxheight}\rangle$ and an erroneous stack by $\langle t, \mathsf{s}^A(\textit{maxheight})\rangle$ ($\mathsf{s}^A(\textit{maxheight})$ points outside of t). For both erroneous and correct stacks, the operation top is always realized in the standard way:

$$\mathsf{top}^A(\langle t, s(i)\rangle) = t[i]$$

On a correct stack the operations push and pop are also realized in the standard way:

$$i \neq \mathsf{s}^A(\textit{maxheight}) \Rightarrow \mathsf{push}^A(x, \langle t, i\rangle) = \langle t[i] := x, \mathsf{s}^A(i)\rangle$$

$$i \neq \textit{maxheight} \Rightarrow \mathsf{pop}^A(\langle t, \mathsf{s}^A(i)\rangle) = \langle t, i\rangle$$

These operations act on an erroneous stack in the following way:

$$\mathsf{push}^A(x, \langle t, \mathsf{s}^A(maxheight)\rangle) = \langle t[maxheight] := x, \mathsf{s}^A(maxheight)\rangle$$

$$\mathsf{pop}^A(\langle t, \mathsf{s}^A(maxheight)\rangle) = \langle t, \mathsf{s}^A(maxheight)\rangle$$

It is important to notice that it is impossible in this realization to make correct an erroneous stack by means of combinations of pushes and pops only.

Let A be the above realization. We equip now the algebra A with the observational equality "$\cong$" defined as the reflexive-symmetric-transitive closure of the following relation "ρ":

1. $\langle t, n\rangle\ \rho\langle t', n\rangle$ if $n \leqslant maxheight$ and $t[i] = t'[i]$ for all $i \leqslant n$.
2. $\langle t, maxheight\rangle\ \rho\langle t', \mathsf{s}^A(maxheight)\rangle$ if t and t' differ only at the index $maxheight$.

Let us show that the set of solutions of any axiom of STACK in the observational algebra $\langle A, \cong\rangle$ defined above is $\mathrm{Val}[X, A]$. This is obvious for the nonerroneous stacks. Consider then a full stack $\langle t, maxheight\rangle$. We check the axiom $\mathsf{top}(\mathsf{push}(x, s)) = x$:

$$\mathsf{top}^A(\mathsf{push}^A(a, \langle t, maxheight\rangle)) = \mathsf{top}^A(\langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle)$$

$$= (t[maxheight] := a)[maxheight] = a$$

We check the axiom $\mathsf{pop}(\mathsf{push}(x, s)) = s$:

$$\mathsf{pop}^A(\mathsf{push}^A(a, \langle t, maxheight\rangle)) = \mathsf{pop}^A(\langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle)$$

$$= \langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle$$

But according to 2: $\langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle \cong \langle t, maxheight\rangle$.

We check now both axioms for an erroneous stack $\langle t, \mathsf{s}^A(maxheight)\rangle$:

$$\mathsf{top}^A(\mathsf{push}^A(a, \langle t, \mathsf{s}^A(maxheight)\rangle)) = \mathsf{top}^A(\langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle)$$

$$= (t[maxheight] := a)[maxheight] = a$$

On the other hand,

$$\mathsf{pop}^A(\mathsf{push}^A(a, \langle t, \mathsf{s}^A(maxheight)\rangle)) = \mathsf{pop}^A(\langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle)$$

$$= \langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle$$

But according to 2 we have

$$\langle t, \mathsf{s}^A(maxheight)\rangle\ \rho\langle t, maxheight\rangle\ \rho\langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle$$

Since "$\cong$" is the reflexive-symmetric-transitive closure of "ρ", we have

$$\langle t, \mathsf{s}^A(maxheight)\rangle \cong \langle t[maxheight] := a, \mathsf{s}^A(maxheight)\rangle$$

In this way we have shown that in $\langle A, \cong \rangle$, the solutions of both axioms of STACK are Val[X, A].

Assume now that we observe the set W_2 of all the ground terms of the form top(t) with t generated by emptystack, push and pop and representing a stack of height least or equal to *maxheight*. It is clear that for two nonerroneous stacks $\langle t, n \rangle$ and $\langle t', n \rangle$ we have

$$\langle t, n \rangle \sim_{W_2} \langle t', n \rangle \quad \text{iff } \langle t, n \rangle \cong \langle t', n \rangle$$

Since an erroneous stack has no observable context, it is indistinguishable with any other stack. Consequently

$$\cong \subseteq \sim_{W_2}$$

and we have shown that $\langle A, \cong \rangle$ is an observational model of the specification $\langle \Sigma_2, \Theta_2, W_2 \rangle$.

The reader has certainly realized that in both examples the corresponding observations have been described in an informal way. In fact in this work we did not deal with a syntax for describing sets of observation terms. It is clear that no syntax may exist allowing to describe (in a finite way) an arbitrary subset of $T_\Sigma(X)$.[8] Consequently the choice of a particular syntax will impose strong restrictions on possible observations. Nevertheless, under such restrictions, we can expect some additional results within this framework.

12. Concluding remarks

We have developed a loose observational semantics of algebraic specifications. We have shown that, under some restrictions, our formalism provides an institution. First, we have investigated how the elements of a carrier of an algebra should be observed through terms. Then we have introduced the concept of observable context underlying our definition of the indistinguishability relation. We have shown that this relation is neither a congruence nor an equivalence relation, in the general case. Both of these results fully agree with our Indistinguishability Assumption. Notice that when we restrict to sort observation, our indistinguishability relation becomes a congruence. Consequently, this notion becomes close to the Nerode congruence [8]. However, unlike in [16], in our approach two observational algebras differing on nonobservable junk do not satisfy the same observational sentences. We do not privilege reachable elements, since this is most suitable for the observational semantics of parametrized specifications in the loose framework (which is one of the topics of further research).

[8] There exist nonrecursive subsets of $T_\Sigma(X)$.

We have introduced in our semantics an additional stage over the indistinguishability relation, namely observational equality. Then we have defined the observational algebras, the observational sentences and the corresponding satisfaction relation. We have shown that the restriction to injective signature morphisms enables our formalism to be extended to an institution.

Acknowledgement

We wish to thank Pippo Scollo for extremely careful readings and many suggestions which helped us to improve technicalities and the language of this paper. This work is partially supported by ESPRIT Working Group COMPASS and CNRS GDR de Programmation.

References

[1] G. Bernot and M. Bidoit, Proving the correctness of algebraically specified software: modularity and observability issues, in: *Proc. 2nd Internat. Conf. on Algebraic Methodology and Software Technology*, Iowa City (1991) 139–161.

[2] G. Bernot and M. Bidoit and T. Knapik, Towards an adequate notion of observation, in: B. Krieg-Brückner, ed., *European Symp on Programming*, Lecture Notes in Computer Science, Vol. 582, Rennes (1992) 39–55.

[3] M. Bidoit, The stratified loose approach: a generalization of initial and loose semantics, in: D. Sannella and A. Tarlecki, eds., *Recent Trends in Data Type Specification*, Lecture Notes in Computer Science, Vol. 332, Gullane (1987) 1–22. Selected papers from the 5th Workshop on Specification of Abstract Data Types.

[4] H. Ehrig, M. Baldamus and F. Orejas, New concepts for amalgamation and extension in the framework of specification logics, in: M. Bidoit and C. Choppy, eds., *Recent Trends in Data Type Specification*, Lecture Notes in Computer Science, Vol. 655, Dourdan (1991) 199–221. Selected papers from the 8th Workshop on Specification of Abstract Data Types.

[5] H. Ehrig and B. Mahr, *Fundamentals of Algebraic Specifications*, EATCS Monographs on Theoretical Computer Science, Vol. 6 (Springer, Berlin, 1985).

[6] J.A. Goguen and R.M. Burstall, Introducing institutions, in: E. Clarke and D. Kozen, eds., *Proc. Logic of Programming Workshop*, Lecture Notes in Computer Science, Vol. 164, Carnegie Mellon (1984) 221–256.

[7] J.A. Goguen and R.M. Burstall, Institutions: abstract model theory for specification and programming, *J. ACM* **39** (1992) 95–146.

[8] J.A. Goguen and J. Meseguer, Persistent interconnection and implementation of abstract modules, in: M. Nielsen and E.M. Schmidt, eds., *ICALP*, Lecture Notes in Computer Science, Vol. 140, Aarhus (1982) 256–281.

[9] J.A. Goguen, J.W. Thatcher and E.G. Wagner, An initial approach to the specification, correctness and implementation of abstract data types, in: R.T. Yeh, ed., *Data Structuring*, Current Trends in Programming Methodology, Vol. 4 (Prentice-Hall, Englewood Cliffs, NJ, 1978) 80–149.

[10] R. Hennicker, Context induction: a proof principle for behavioural abstractions and algebraic implementations, *Formal Aspects Comput.* **3** (1991) 326–345. Also available as MIP-9001 report, Fakultät für Mathematik und Informatik, Universität Passau.

[11] R. Hennicker and M. Wirsing, Observational specification: a Birkhoff theorem, in: H.-J. Kreowski, ed., *Recent Trends in Data Type Specification*, Selected papers from the 3rd Workshop on Theory and Applications of Abstract Data Types, Informatik Fachberichte 116, Bremen (1985) 119–135. Also available as MIP-8508 report, Fakultät für Mathematik und Informatik, Universität Passau.

[12] S. Kamin, Final data types and their specification, *ACM Trans. Prog. Lang. Syst.* **5** (1983) 97–123.
[13] T. Knapik, Specifications with observable formulae and observational satisfaction relation, in: M. Bidoit and C. Choppy, eds., *Recent Trends in Data Type Specification*, Lecture Notes in Computer Science, Vol. 655, Dourdan (1991) 271–291. Selected papers from the 8th Workshop on Specification of Abstract Data Types.
[14] T. Knapik, Spécifications algébriques observationnelles modulaires: une sémantique fondée sur une relation de satisfaction observationnelle, Ph.D. Thesis, Université de Paris-Sud, 1993.
[15] J. Meseguer and J.A. Goguen, Initially, induction and computability, in: M. Nivat and J.C. Reynolds, eds., *Algebraic Methods in Semantics* (Cambridge Univ. Press, Cambridge, 1985) 459–541.
[16] P. Nivela and F. Orejas, Initial behaviour semantics for algebraic specification, in: D. Sannella and A. Tarlecki, eds., *Recent Trends in Data Type Specification*, Lecture Notes in Computer Science, Vol. 332, Gullane (1987) 184–207. Selected papers from the 5th Workshop on Specification of Abstract Data Types.
[17] F. Orejas, M. Navarro and A. Sànches, Implementation and behavioural equivalence: a survey, in: M. Bidoit and C. Choppy, eds., *Recent Trends in Data Type Specification*, Lecture Notes in Computer Science, Vol. 655, Dourdan (1991) 193–125. Selected papers from the 8th Workshop on Specification of Abstract Data Types.
[18] H. Reichel, Behavioural equivalence – a unifying concept for initial and final specification methods, in: *3rd Hungarian Comput. Sci. Conf.*, Budapest (1981) 27–39.
[19] H. Reichel, Behavioural validity of conditional equations in abstract data types, in: *Contributions to General Algebra, Vol 3, Proc. Vienna Conf.* (1984) 301–324.
[20] A. Salibra and G. Scollo, A soft stairway to institutions, in: M. Bidoit and C. Choppy, eds., *Recent Trends in Data Type Specification*, Lecture Notes in Computer Science, Vol. 655, Dourdan (1991) 310–329. Selected papers from the 8th Workshop on Specification of Abstract Data Types.
[21] D. Sannella and A. Tarlecki, On observational equivalence and algebraic specification, *J. Comput. System Sci.* **34** (1987) 150–178.
[22] D. Sannella and M. Wirsing, A kernel language for algebraic specification and implementation, Tech. Report CSR-131-83, Department of Computer Science, University of Edinburgh, 1983. Extended abstract in Proc. *Internat. Conf. on Foundations of Computation Theory*, Lecture Notes in Computer Science, Vol. 158, Borgholm (1983) 413–427.
[23] N.W.P. van Diepen, Implementation of modular algebraic specifications, in: H. Ganzinger, ed., *European Symp. on Programming*, Lecture Notes in Computer Science, Vol. 300, Nancy (1988) 64–78.
[24] M. Wirsing, Algebraic specification, in: J. van Leeuwen, ed., *Formal Models and Semantics*, Handbook of Theoretical Computer Science, Vol. B (Elsevier, Amsterdam, 1990) 675–788.